antek networks INC.

User Manual

of

EGW Series
VSP Series
WRG Series
Gateway

Version 1.1

May 22, 2003

7F-3, No. 3, Lane 99, Puding Rd, HsinChu 300, Taiwan, R.O.C.
TEL: +886-3-516-0139 Fax: +886-3-516-0193
http://www.antek.com.tw
Email: service@antek.com.tw

EGW-802 /S/A

2-Port Voice Gateway, 1 Ethernet port

EGW-804 /S/A/B/C

4-Port Voice Gateway, 1 Ethernet port

VSP-5002 /S/A

2-Port VoiceShaper Gateway, 2 Ethernet port

VSP-5004 /S/A/B/C/GK/SGK/AGK

4-Port VoiceShaper Gateway, 5 Ethernet port
Embedded GateKeeper was option

VSP-2500

16-Port VoiceShaper Gateway +EmbeddedGatekeeper

WRG-5002 /S/A

2 port VoiceShaper Gateway

WRG-5004 /S/A/B/C

2 port VoiceShaper Gateway

Model	FXO Port	FXS Port	LAN Port	WAN Port	Gatekeeper	Bandwidth Control	NAT	Access Point	Size
EGW-802	2	X	1	X	X	X	X	X	Compact
EGW-802S	X	2	1	X	X	X	X	X	Compact
EGW-802A	1	1	1	X	X	X	X	X	Compact
EGW-804	4	X	1	X	X	X	X	X	Compact
EGW-804S	X	4	1	X	X	X	X	X	Compact
EGW-804A	2	2	1	X	X	X	X	X	Compact
EGW-804B	3	1	1	X	X	X	X	X	Compact
EGW-804C	1	3	1	X	X	X	X	X	Compact
VSP-5002	2	X	1	1	X	√	√	X	Compact
VSP-5002S	X	2	1	1	X	√	√	X	Compact
VSP-5002A	1	1	1	1	X	√	√	X	Compact
VSP-5004	4	X	4	1	X	√	√	X	Compact
VSP-5004S	X	4	4	1	X	√	√	X	Compact
VSP-5004A	2	2	4	1	X	√	√	X	Compact
VSP-5004B	3	1	4	1	X	√	√		Compact
VSP-5004C	1	3	4	1	X	√	√	X	Compact
VSP-5004GK	4	X	4	1	√	√	√	X	Compact
VSP-5004SGK	X	4	4	1	√	√	√	X	Compact
VSP-5004AGK	2	2	4	1	√	√	√	X	Compact
VSP-2500	0-16	0-16	1	1	√	√	X	X	1u
				Modules for VSP-2500 selection					
VM-402	4								Module
VM-401S		4							Module
VM-442S	2	2							Module
WRG-5002	2	X	1	1	X	X	√	√	Compact
WRG-5002S	X	2	1	1	X	X	√	√	Compact
WRG-5002A	1	1	1	1	X	X	√	√	Compact
WRG-5004	4	X	4	1	X	X	√	√	Compact
WRG-5004S	X	4	4	1	X	X	√	√	Compact
WRG-5004A	2	2	4	1	X	X	√	√	Compact
WRG-5004B	3	1	4	1	X	X	√	√	Compact
WRG-5004C	1	3	4	1	X	X	√	√	Compact

Table 1. Model-Function Matrix

Note:

1. **FXO port: line port, connecting to the PSTN line.**
2. **FXS port: phone port, connecting to an analog phone set.**

© Copyright 2003
antek networks INC.

1. Copyright Notice

antek networks INC. is a registered trademark of antek networks INC. Other referenced trademarks are trademarks (registered or otherwise) of the respective trademark owners. No part of this document may be reproduced, stored, or transmitted in any form by any means without the prior written permission of antek networks INC.

Information furnished herein by antek networks INC., is believed to be accurate and reliable. The authors have used their best efforts in preparing this material. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness, however, antek networks INC. assumes no liability for errors in this document, or for liability otherwise arising from the application or use of any such information or for any infringement of patents or other intellectual property rights owned by third parties, which may result from such application or use.

The products, their specifications, and the information appearing in this document are subject to change without notice.

Printed in Taiwan, R.O.C.

©2003 by antek networks INC., all rights are reserved.

Table of Contents

1 **1. Copyright Notice 4**

2 **2. Introduction 8**

3 **3. Safety Information 11**

4 **4. Package contents 12**

5 **5. Device installation 13**

5.1 Interface Definition 21
5.2 LED Indicators (Table 2) 21

6 **6. Connection Example 22**

6.1 Connect through Ethernet Hub: (VSP-2500, VSP-Series) 22
6.2 Direct Connect through Crossover Ethernet line: (VSP-2500, VSP-Series) 22
6.3 Direct Connect: (VSP-5004) 23
6.4 Direct Connect: (EGW-Series) 24
6.5 Wireless VoIP Gateway Application: (WRG-5000 Series) 25

7 **7. Configuring gateway through RS232 serial port 26**

8 **8. Set Network Parameters 29**

9 **9. Using Web Browser To Configure Gateway System 30**

9.1 Connecting to the gateway from web browser 30
9.2 Change configuration of the system 31
9.2.1 Gateway System Maintenance 32
9.3 Gateway Configuration 33
9.3.1 Product Version 33
9.3.2 Network Parameters 34
9.3.2.1 Settings for Console/Telnet only 35
9.3.3 H323 Configuration 36
9.3.3.1 Gatekeeper related functions 37
9.3.3.2 Embedded Gatekeeper On (for Gatekeeper model) 38
9.3.3.2.1 Set Allowed Registration Constraint (for Gatekeeper model) 39
9.3.3.2.2 Set Pre-Allowed Registration Endpoints (for Gatekeeper model) ... 41
9.3.3.2.3 Display Registered Endpoints (for Gatekeeper Model) 44
9.3.3.2.4 Disable The Gatekeeper Function (for Gatekeeper model) 46
9.3.4 SIP Usage Guide (Settings for Console/Telnet) 48
9.3.4.1 SIP Configuration 48
9.3.4.2 Direct dialing plan for SIP 49

9.3.5 Phone/Line Dialing Plan 50
9.3.5.1 Phone Dialing Plan (EGW-802S, EGW-804S, VSP-5002S/5004S, VSP2500) 50
9.3.5.1.1 Representation Number 51
9.3.5.2 Phone/Line Dialing Plan (VSP-2500 only) 51
9.3.5.2.1 Representation Number 53
9.3.5.3 Phone/Line Dialing Plan (EGW-802, EGW-804, VSP-5002/5004, WRG-5002/5004 gateways with line ports) 54
9.3.5.3.1 Representation Number 55
9.3.5.3.2 Connect to PSTN through PBX 55
9.3.5.3.3 Extension Number Connected through PBX 55
9.3.5.3.4 Delete Extension 56
9.3.5.3.5 Settings for Console/Telnet only 56
9.3.6 Hot Line Calls 57
9.3.6.1 Settings for Console/Telnet only 58
9.3.7 Direct Call 59
9.3.8 Show All Numbering Plan 61
9.3.9 Voice processing control 62
9.3.9.1 Settings for Console/Telnet only 64
9.3.10 Gateway Access Control 65
9.3.10.1 Settings for Console/Telnet only 66
9.3.11 Advanced Configurations 67
9.3.11.1 Settings for Console/Telnet only 69
9.3.11.2 Line Port (FXO) Characteristics 70
9.3.11.3 Phone Port (FXS) Characteristics 70
9.3.12 Extended Configurations 71
9.3.13 Voice calls Monitoring 74
9.3.14 CDR Server 75
9.3.15 IP Sharing/GW Stack-ability (VSP-Series only) 76
9.3.15.1 Stackable GWs 77
9.3.15.2 IP Sharing (1 IP Address Only) 78
9.3.15.3 IP Sharing (more than 1 IP Address available) 79
9.3.15.4 IP-Sharing Management and Maintenance 80
9.4 Bandwidth Control (VSP-Series only) 81
9.4.1 Enable/Disable Bandwidth Control. 81
9.4.2 Set Packet Shaping Mode. 82
9.4.3 Set WAN Inbound/Outbound Bandwidth. 83
9.4.4 Set Inbound/Outbound Packet Shaping Jitter. 84
9.4.5 Set Shaping Conditions. 85
9.4.6 Set Priority Queue Bandwidth. 86
9.4.7 Display Queue Traffics 88
9.4.8 Display Application Traffics 90
9.4.9 Display Top Network Users. 92
9.4.9.1 LAN Top Network User 92
9.4.9.2 WAN Top Network User 94
9.4.10 Traffic History 96

9.4.11 Configuration Examples: 97
9.5 Run Telnet 100
9.6 Help 101
9.7 NAT Setting (VSP-5004/5002/WRG-5004 only) 102
9.7.1 NAT Enable Control 102
9.7.2 LAN Port Network Parameters Settings 103
9.7.3 Virtual Server Control 104
9.7.4 Virtual Servers 105
9.7.5 DHCP Enable Control Mode 106
9.7.6 DHCP Server Control 107
9.7.7 DHCP Server Status 108
9.8 Q.931 and RAS port numer adjustment (Telnet / Console setting only) 108
9.9 Wireless LAN Access Point Setting (WRG-5000 series devices only) .. 109

10 **Feedback 110**

11 **Size of setting data (Table 3.) 111**

12 **Appendix A: Terminology Index 112**

13 **Appendix B: Specification 115**

2. Introduction

This user manual includes three series of VoIP gateways.

1. The first is EGW-series gateway, which has only one Ethernet interface and 1-4 analog ports to provide all general VoIP gateway functions.
2. The second is VSP-5004 series gateway, which has five Ethernet interfaces (four are LAN ports, one is WAN interface) and 2-4 analog ports to provide not only general VoIP gateway functions but also general bandwidth control and NAT (Network Address Translation) functions to solve shortage of IP addresses.
3. The third is VSP-2500 series gateway, which has two Ethernet interfaces (one is LAN, another is WAN interface) and 2-16 analog ports to provide not only general VoIP gateway functions but also general bandwidth control functions that can guarantee the good voice quality.

The VoIP series gateways are advanced gateway systems that allow users to achieve perfect voice/fax communication over the IP network. A telephone, fax machine, PBX, key telephone system, or the PSTN line can be directly connected to the gateway and gain the benefit of Voice over IP immediately without any additional software or complex configuration required.

The VoIP series gateways have perfectly made the integration of both data and voice traffic over a single data network possible. As voice signals are compressed by efficient audio CODECs (such as G.723.1 or G.729AB), they will take only a few bandwidth of original data network.

Furthermore, in order to provide superior voice quality over quality varying IP network, it is equipped with advanced Quality of Service (QoS) technologies, enhanced jitter buffering, lost packets recovering, echo cancellation and packet delay reconstruction. Therefore, it supports reliable voice/fax communication over congested IP network.

The **major problem** of other VoIP gateways (or IP phone) used in an office is that they are using the same link (leased line or ADSL) as used by data traffics to connect to Internet. Because of this shared bandwidth media, the VoIP packets could be easily affected by the office's data traffics to cause a lot of voice delay and voice chopping. For example, in a 64 kbps link, a single 1514 bytes data packet can induce nearly 200 ms delay. And in a general ftp/web application, the VoIP packets could be easily delayed by more than five 1514 bytes data packets to generate more than 1 second voice delay. Worst of all is that this delay is random, thus causing jittered voice packets. These jittered packets will finally generate the chopped voice.

The **major goal** of the VSP-series gateway is to solve this problem to let a single IP network link work well for both data traffics and VoIP traffics. In order to finish this job, the VSP-series gateway is supporting both the VoIP gateway functions and bandwidth control/packet shaping functions. It has the general VoIP gateway functions to let PBX extensions share the VoIP services without changing any dialing procedures. It also has the general bandwidth control/packet shaping functions to control the bandwidths of particular applications or workstations. Better than these two functions separated are that the VSP-Series can dynamically adjust the available bandwidth for data traffics according to really used VoIP traffics. The VoIP calls do not need to reserve a fixed rate bandwidth; since voice packets could be off any time when talker is silent. The VSP-Series makes full advantage of combining these two functions together and do both jobs excellently to guarantee the best voice quality and the best bandwidth usage that could not be done if these two functions were separated.

The series of gateways also have some other features that make it **Very Special:**

1. Embedded Gatekeeper (Refer Table 1 for supported models)

The VoIP gateway has embedded gatekeeper functions that can be enabled or disabled, if enabled it is doing both a VoIP gateway functions and the Gatekeeper functions. All the general gateway functions are not affected by the enabled gatekeeper functions. The gatekeeper when integrate with the gateway will support the following three functions:

1. Grouping function – the gatekeeper can manage upto 32 independent groups of gateways.
2. Hunting group function – the gatekeeper can support hunting functions that will hunt available ports among many gateways.
3. Gatekeeper backup function – all the gateways can have a primary and a secondary gatekeeper to enable the gatekeeper backup function.

2. NAT pass-through

All the VoIP gateways can be configured to pass-through general NAT devices. The NAT devices do not need to provide additional functions to support VoIP service. This unique function will let the VoIP gateways work fine inside any office.

3. Bandwidth control (VSP-Series only)

The VSP-series gateway, when putting between the office network and the WAN link, can control the bandwidth of all the data traffics passing through it, and can reserve enough bandwidth for VoIP traffics needs, thus guarantee the voice quality.

4. IP sharing/stackability (VSP-Series only)

The VSP-series gateway can be configured to share a single IP address with other workstations or NAT devices. In some offices, the public IP addresses are very scarce; it's hard to find other available IP addresses for additional network devices. The VSP-series gateway can ease the MIS manager by using the same IP address used by other workstation or NAT devices and let them both work well.

5. CDR recording

The VoIP gateway can generate detailed call records of the VoIP calls and send them to a CDR server. The CDR server will collect these records and can generate/sorting CDR reports based on the calling/called gateways, call duration, calling/called numbers, ... etc.

6. Other advanced VoIP gateway

The VoIP gateway has many other advanced gateway functions, such as PPPoE and DHCP for dynamic IP allocation, adaptive PBX busy disconnection, hot line function, robust voice processing against heavy packet loss, gateway security control, DSP codec selection, H.323 flexible interoperability, ... etc. These additional advanced functions make sure the VoIP gateway is the best choice in the VoIP world.

The purpose of this user manual is to give user a detailed installation and configuration guide. For a first time user, please follow the installation procedure in section 4 to install this gateway. This product is designed to support as many applications as possible, but with configurations as simple as possible. In order to ease the system configurations, web browser could do all settings except the initial installation stage.

3. Safety Information

The most careful attention has been devoted to quality standards in the manufacture of the Gateway. Safety is a major factor in the design of every set. But, safety is your responsibility too.

- Use only the required power voltage.

Power Input: AC 100-240V, 50-60Hz

- To reduce the risk of electric shock, do not disassemble this product. Opening or removing covers may expose the Gateway to hazardous voltages. Incorrect reassembly can cause electric shock when this product is subsequently used.

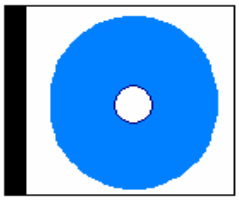
- Never push objects of any kind into the equipment through housing slots since they may touch hazardous voltage points or short out parts those could result in a risk of electric shock. Never spill liquid of any kind on the product. If liquid is spilled, please refer to the proper service personnel.

- Use only Unshielded Twisted Pair (UTP) Category 5 Ethernet cable to RJ-45 port of the Gateway.

4. Package contents

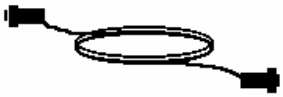
Make sure the following contents are included in the package
1 Unit – Gateway product (please check with your order)
1 Unit – Power cord (or power adapter depends on your order model)
1 Unit – RS-232 cable
1 Unit – User Manual CD

One Gateway Box



User Manual CD

Power cord

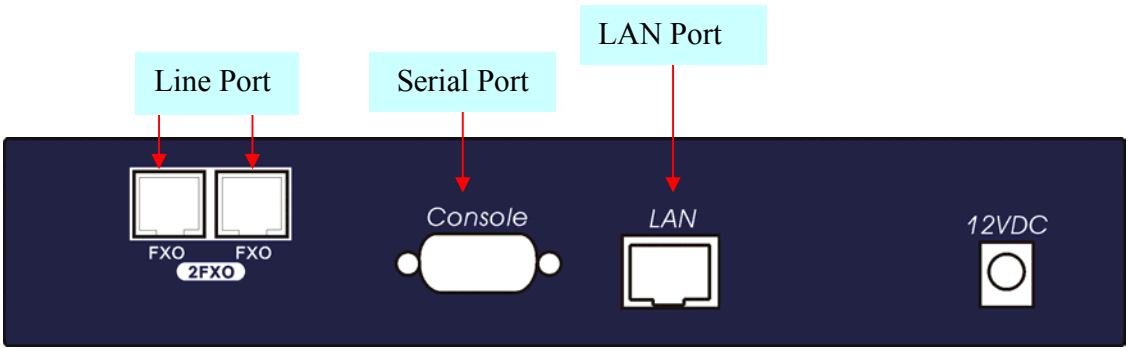


RS-232 cable

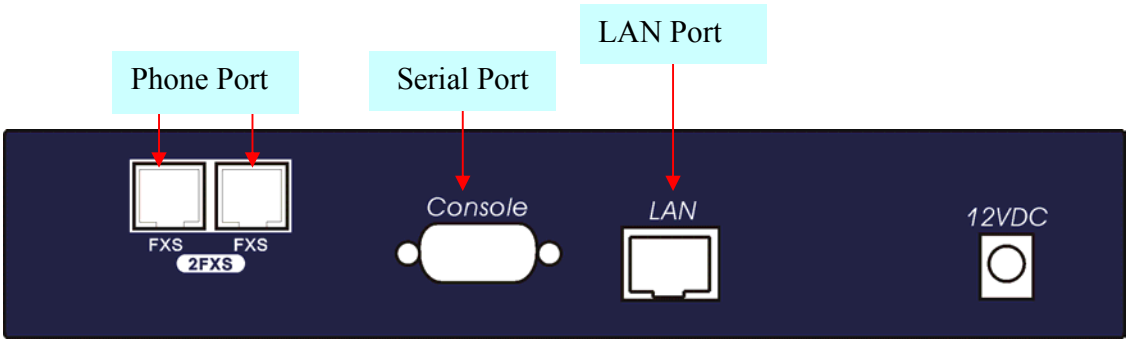
5. Device installation

1. Unpack all contents of the Gateway package.
2. Connect the Local Area Network (LAN) cable to the RJ-45 port at the front of the Gateway as shown in the following figure.
3. Connect the Power Cord to the 100-240V at the back of the Gateway.
4. Connect the Power Cord to the AC-Outlet.
5. Connect a phone set to the **phone port** or connect a PSTN line/PABX extension line to the **Line port** with RJ-11 cable.
6. Connect the RS-232 cable to PC's serial port. (1st time configuration), please refer to section 7 for the settings of serial port.
7. Power on Gateway and start to configure it.

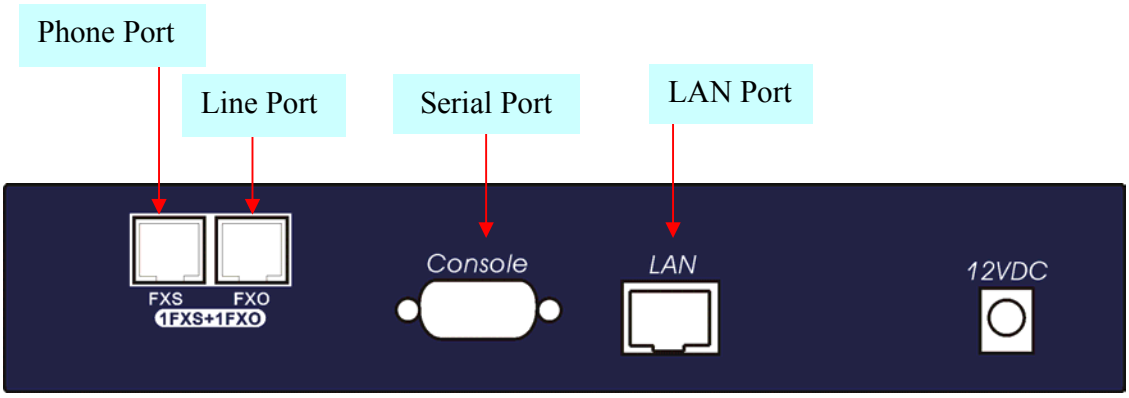
EGW Series Device panel of the voice gateway:



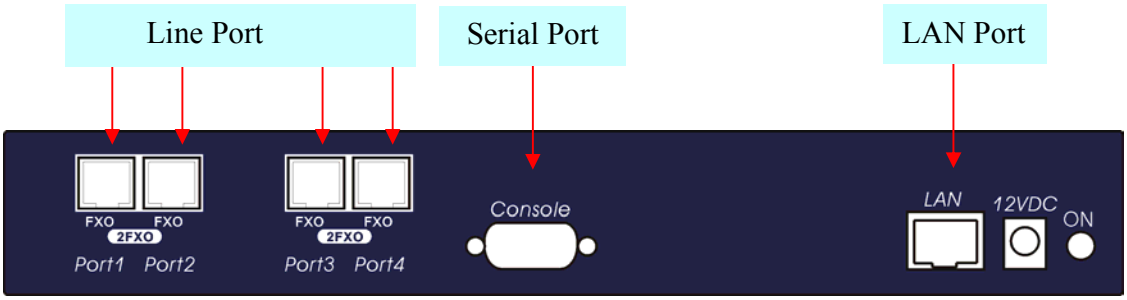
EGW-802



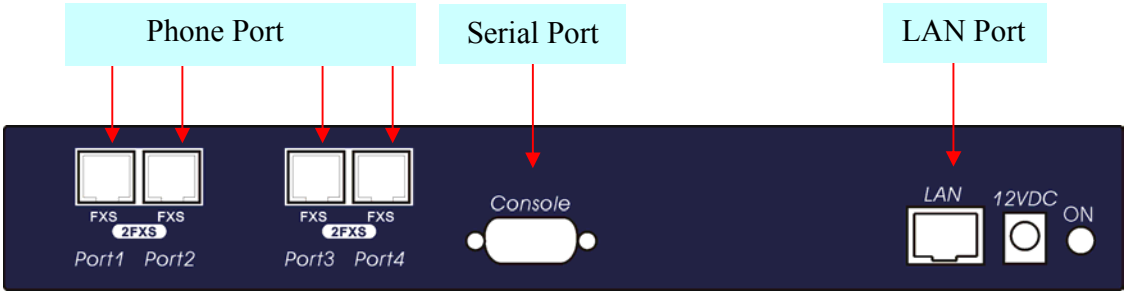
EGW-802S



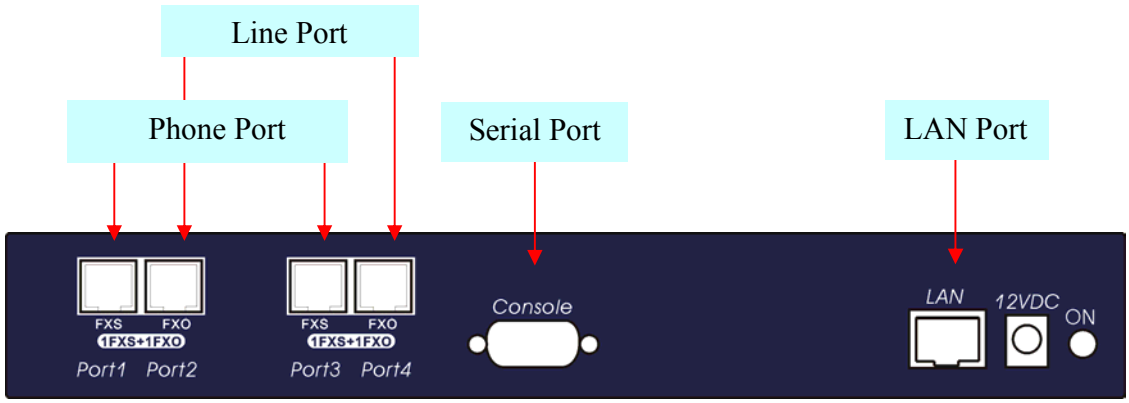
EGW-802A



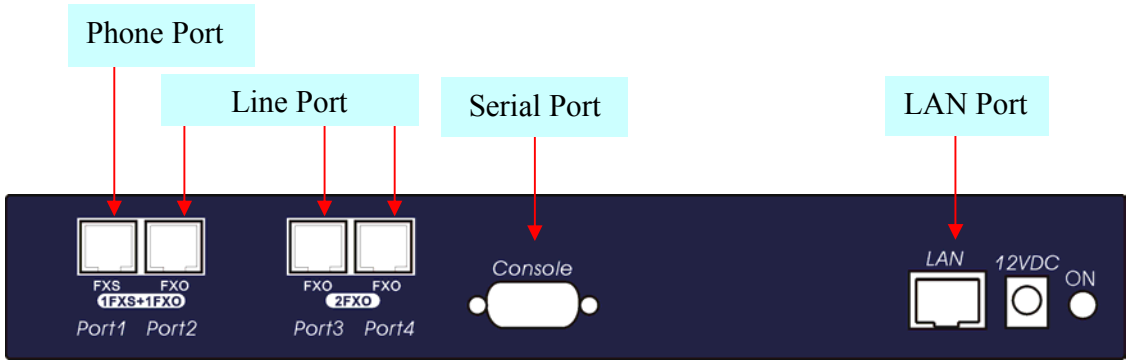
EGW-804



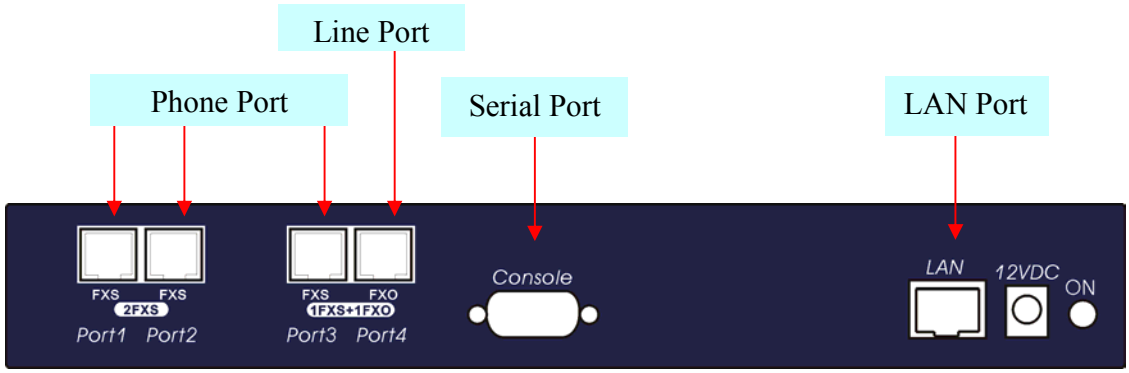
EGW-804S



EGW-804A



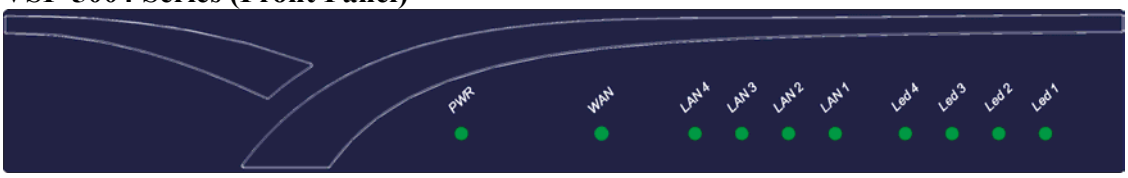
EGW-804B

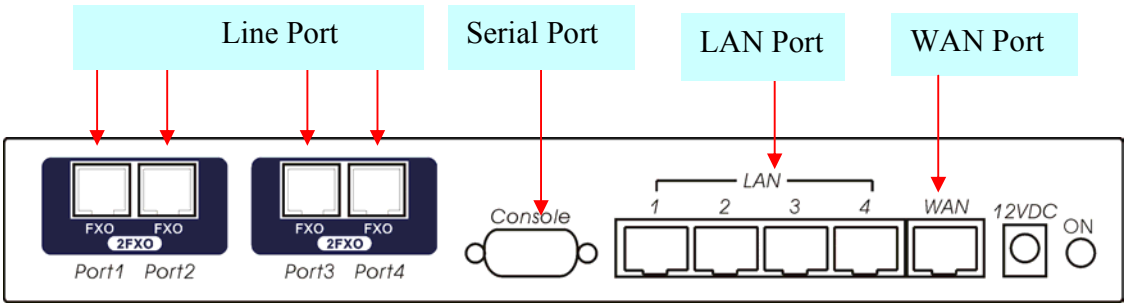


EGW-804C

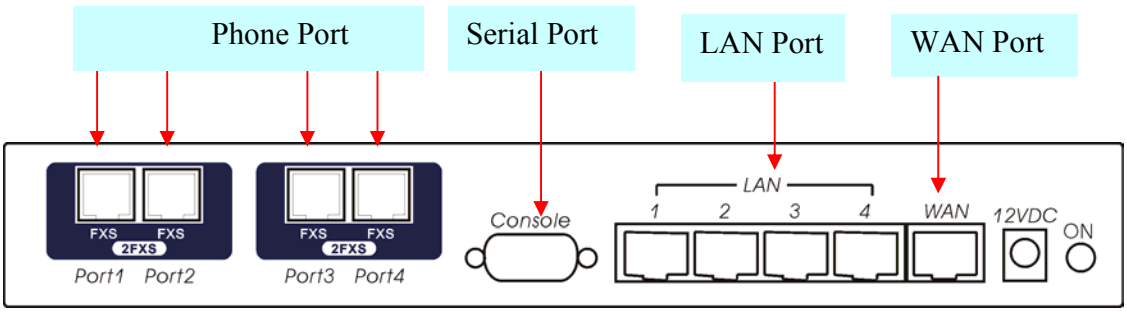
VSP Series Device panel of VoiceShaper Gateway:

VSP-5004 Series (Front Panel)

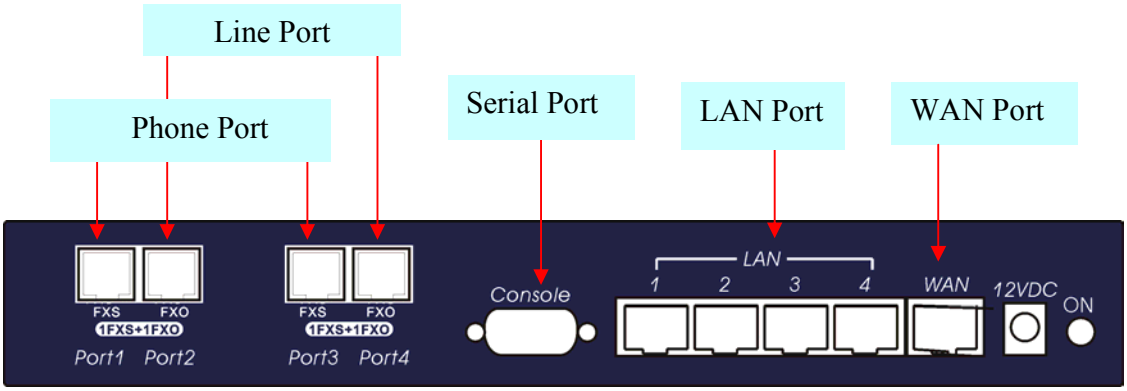




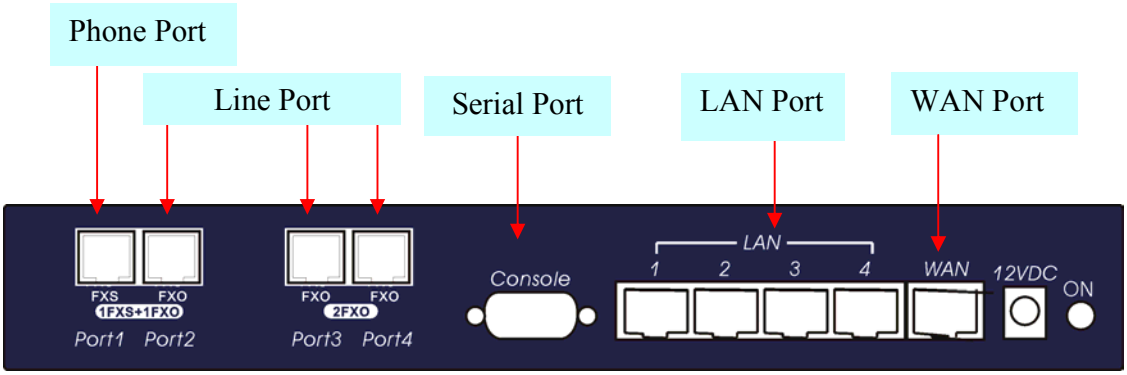
VSP-5004



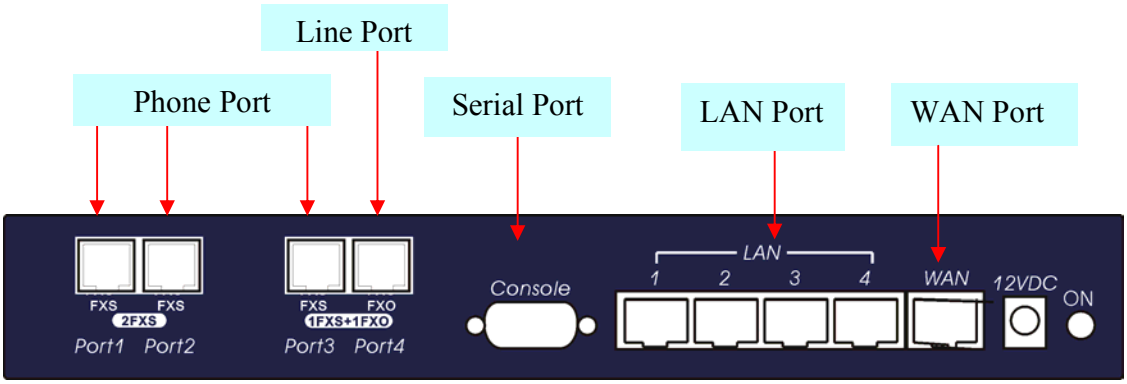
VSP-5004S



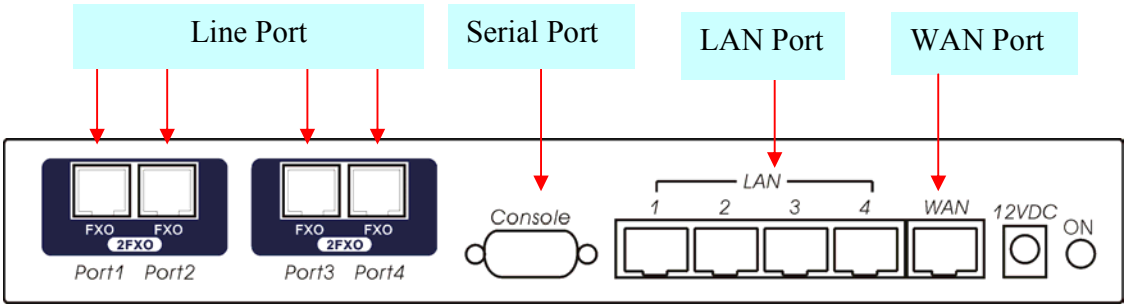
VSP-5004A



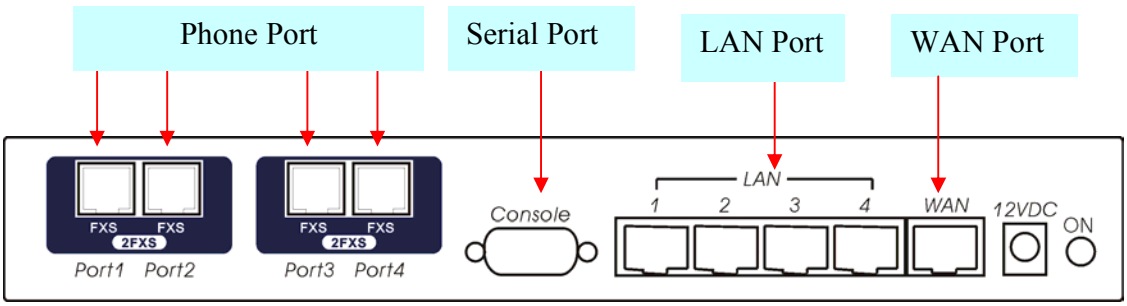
VSP-5004B



VSP-5004C

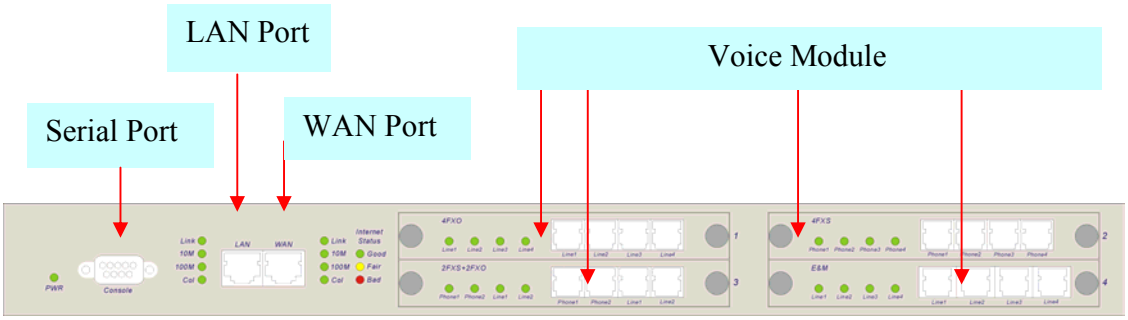


VSP-5004GK



VSP-5004SGK

VSP-2500 System



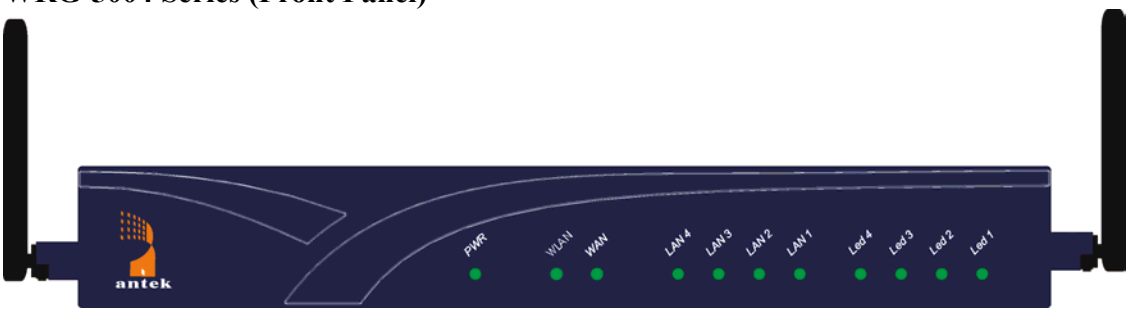
VSP-2500

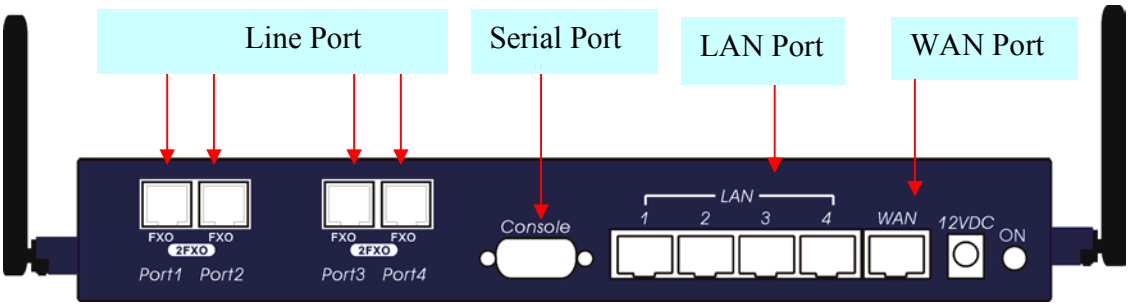
VSP-2500 has 4 slots that can support 1 to 4 analog port modules. Each module offers 4 analog ports.

VM-402: 4 FXO ports module
VM-401S: 4 FXS ports module
VM-442S: 2 FXO + 2 FXS ports module

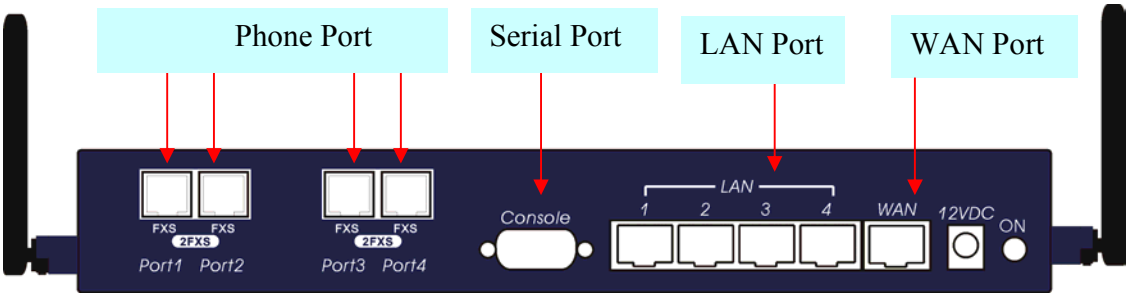
WRG Series Device panel of Wireless Gateway:

WRG-5004 Series (Front Panel)

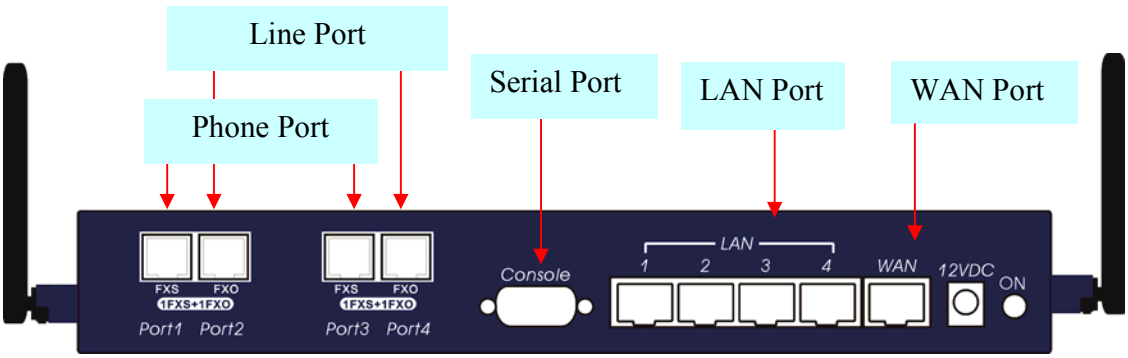




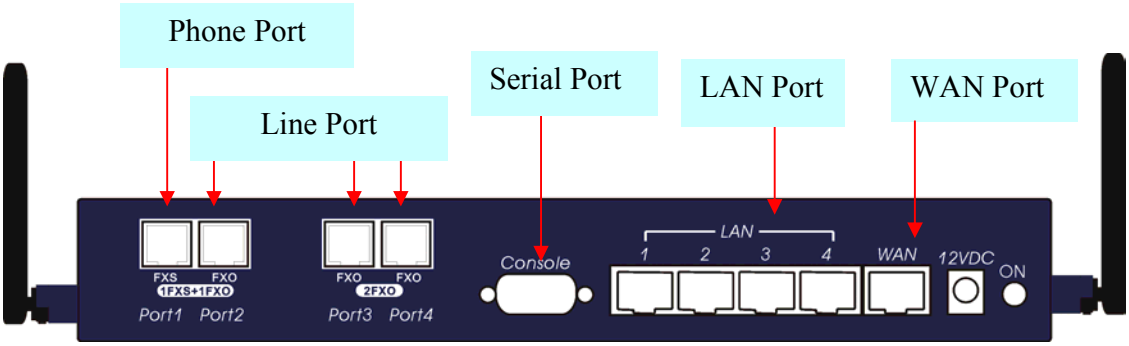
WRG-5004



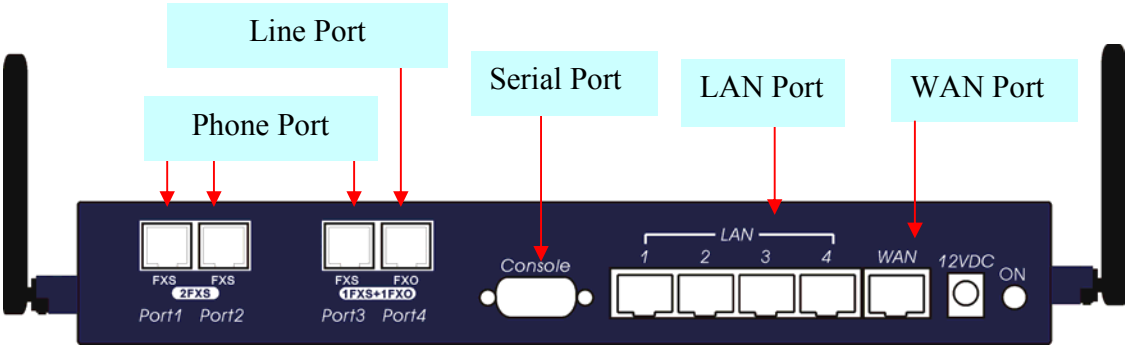
WRG-5004S



WRG-5004A



WRG-5004B



WRG-5004C

5.1 Interface Definition

CONSOLE

It is a RS-232 communication port, and connected to the PC's serial port.

LINE1 to LINE4

To be connected to PSTN line (RJ-11 connector)

Phone1 to Phone4

To be connected to analog phone set (RJ-11 connector)

LAN

To be connected to internal LAN network (RJ-45 connector).

WAN

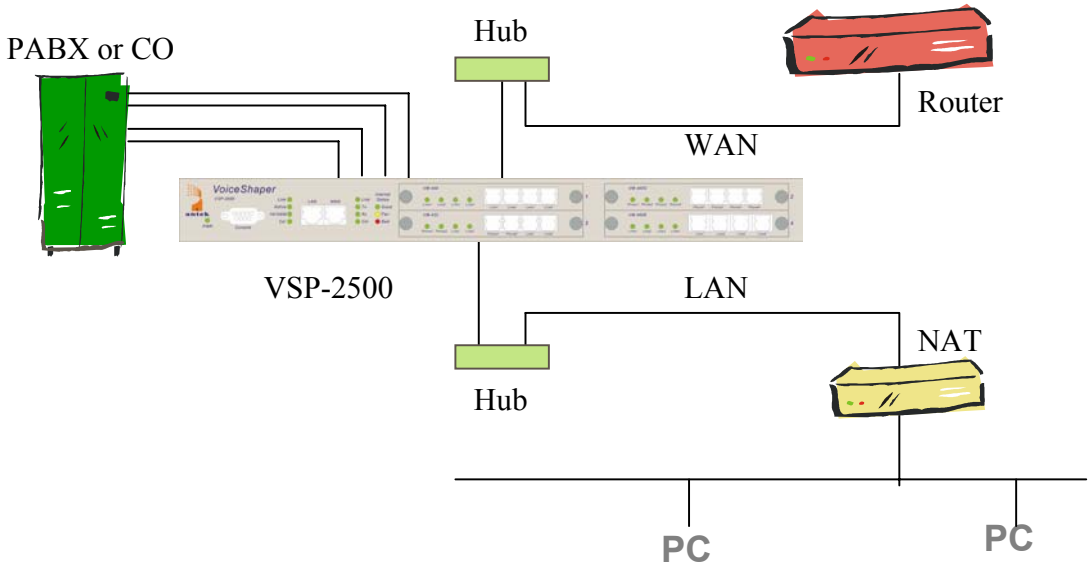
To be connected to external WAN network (RJ-45 connector).

5.2 LED Indicators (Table 2)

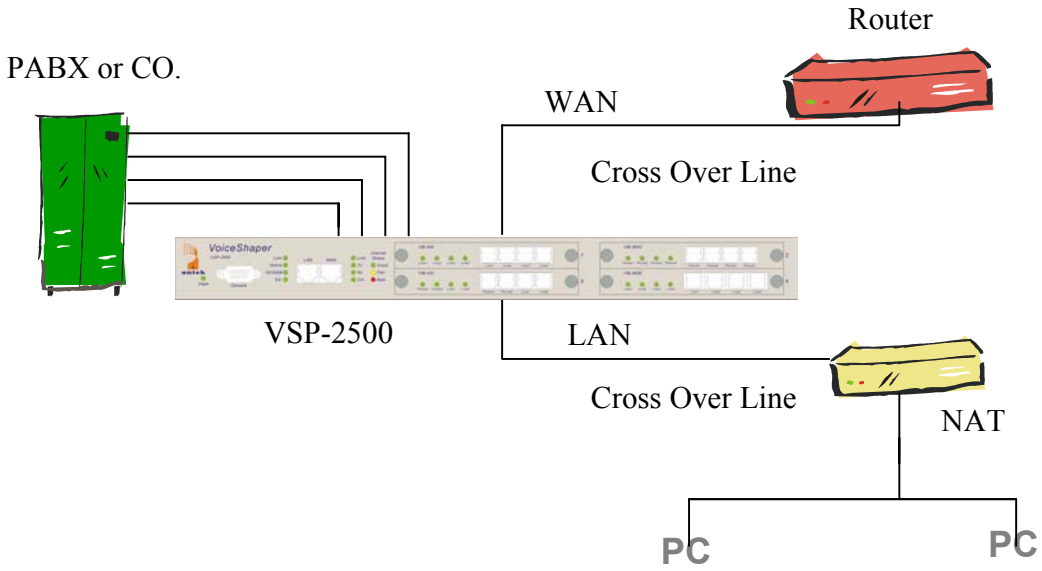
LED	Green light	Activity
Active	ON	LAN is receiving/transmitting data
Col	ON	The data packets have collisions during transmission
Link	ON	Network connection is OK
LINE1	ON	Connected to PSTN line
LINE2	ON	Connected to PSTN line
LINE3	ON	Connected to PSTN line
LINE4	ON	Connected to PSTN line
Phone1	ON	Connected to phone set
Phone2	ON	Connected to phone set
Phone3	ON	Connected to phone set
Phone4	ON	Connected to phone set
POWER	ON	Power is on
RX	ON	Receiving data from network
TX	ON	Data is being transmitted to network
10/100M	ON	When "***Link***" is on, the network data transmission speed is 100Mps
10/100M	OFF	When "***Link***" is off, the network data transmission speed is 10Mps
Bad	ON	Internet connection speed is bad (VSP-2000 only)
Fair	ON	Internet connection speed is fair (VSP-2000 only)
Good	ON	Internet connection speed is good (VSP-2000 only)

6. Connection Example

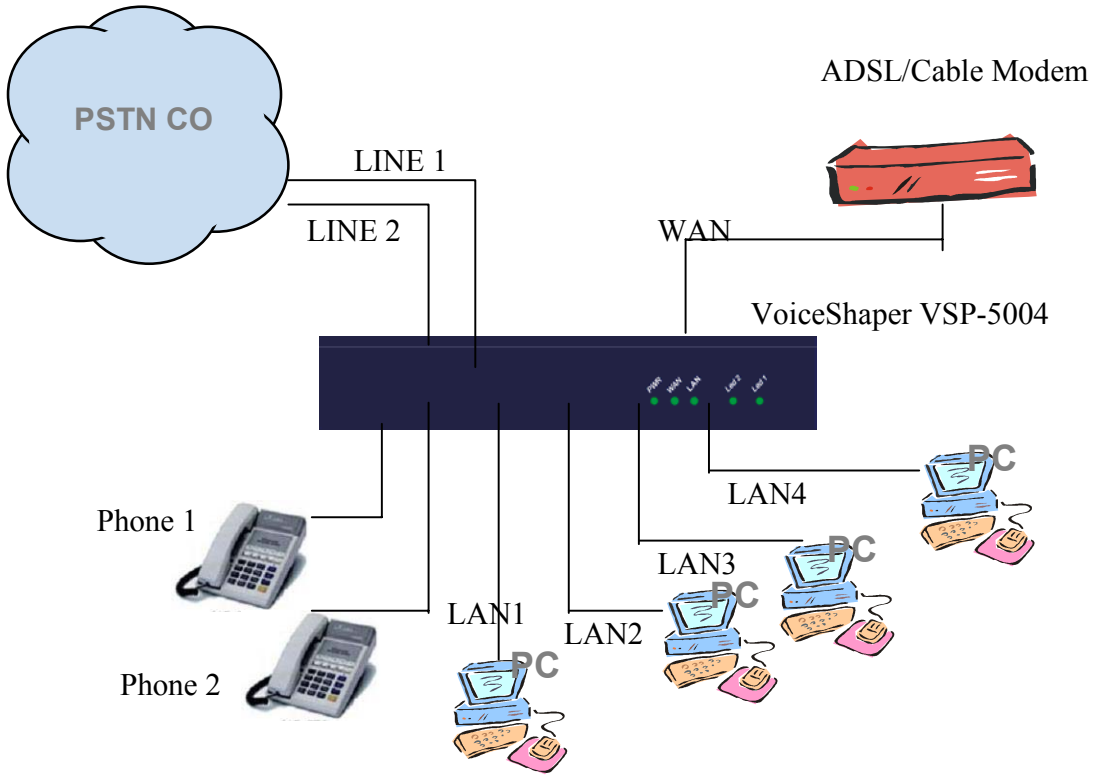
6.1 Connect through Ethernet Hub: (VSP-2500, VSP-Series)



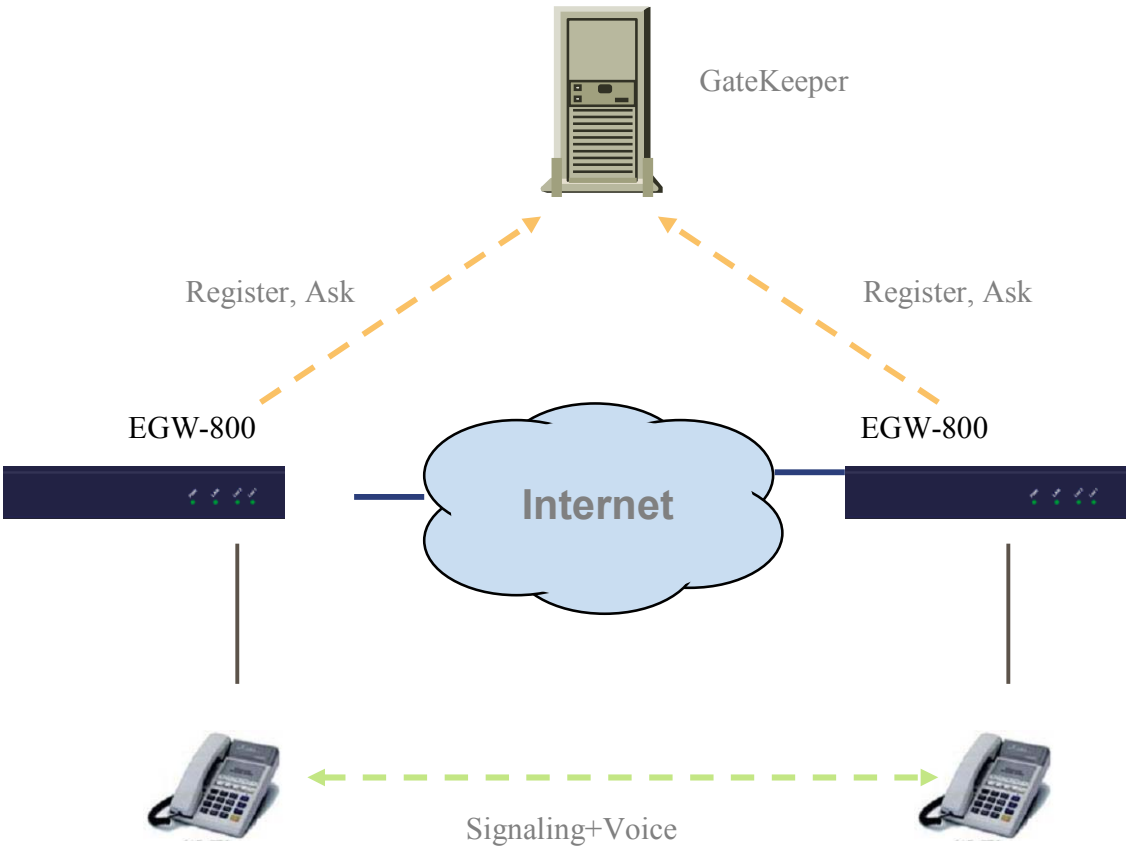
6.2 Direct Connect through Crossover Ethernet line: (VSP-2500, VSP-Series)



6.3 Direct Connect: (VSP-5004)

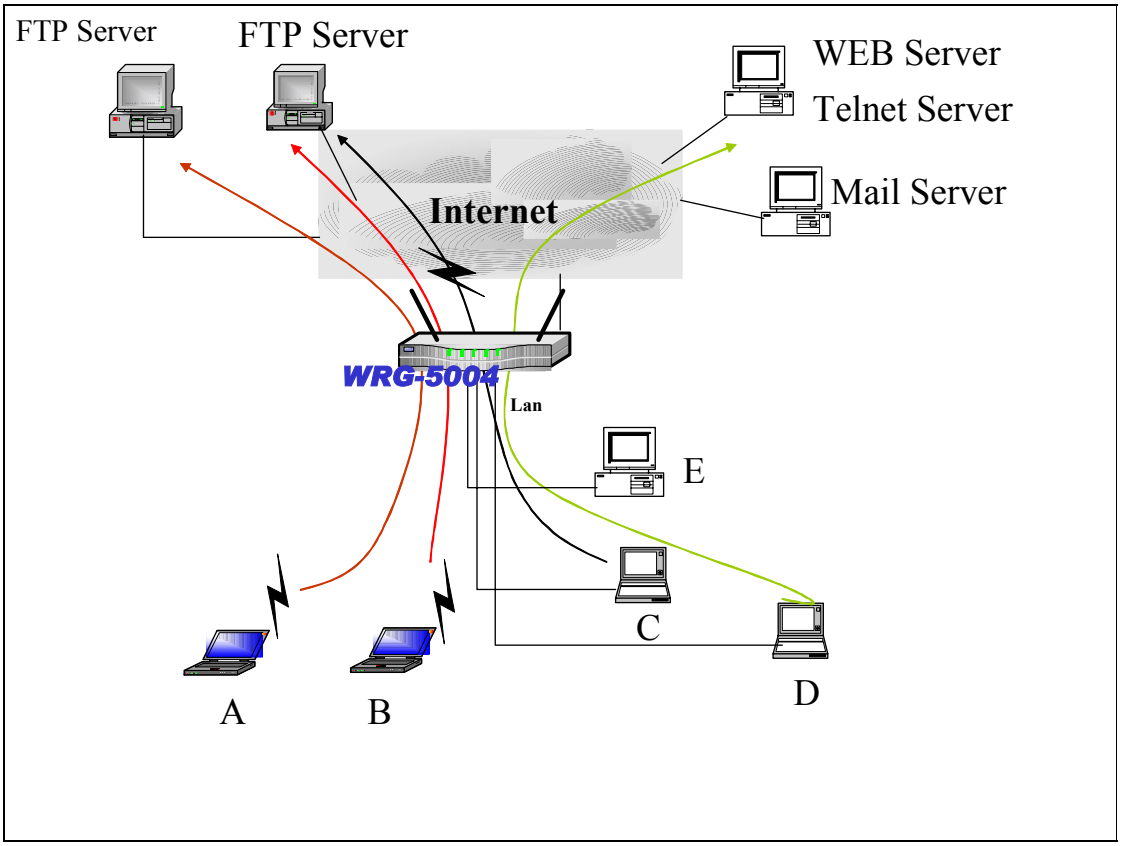


6.4 Direct Connect: (EGW-Series)

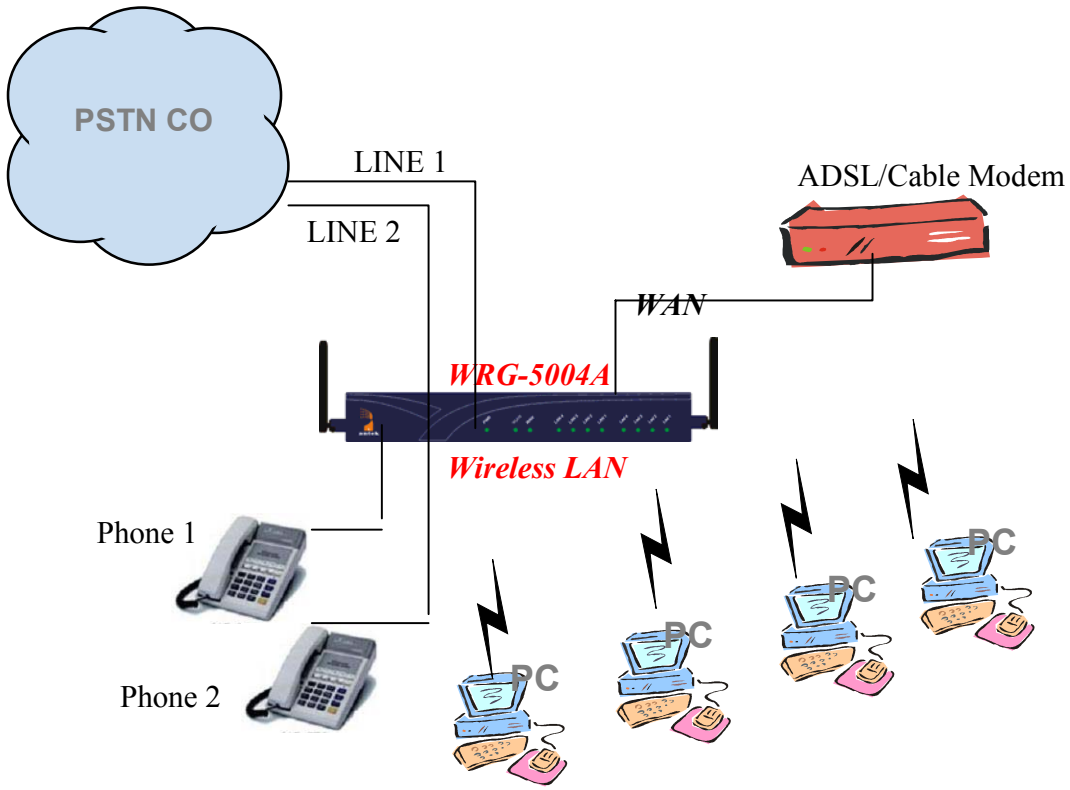


6.5 Wireless VoIP Gateway Application: (WRG-5000 Series)

Application 1 for wireless network:



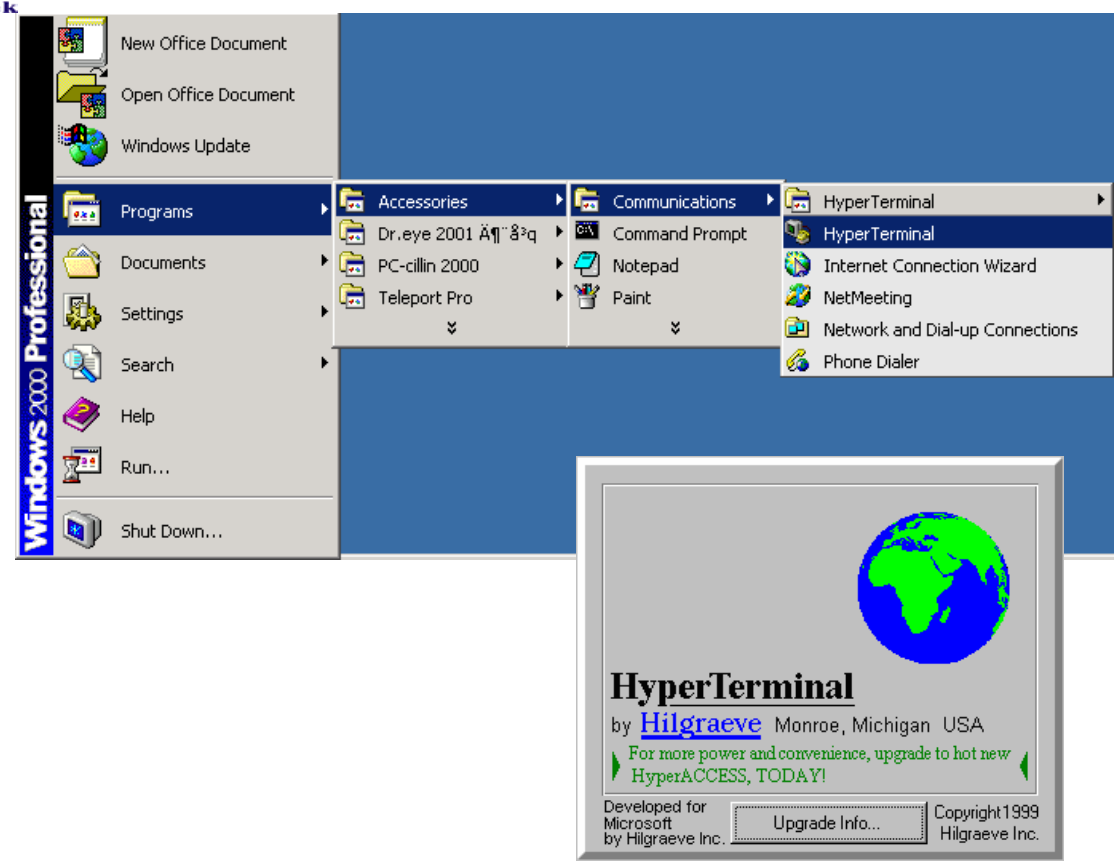
Application 2 for VoIP network:

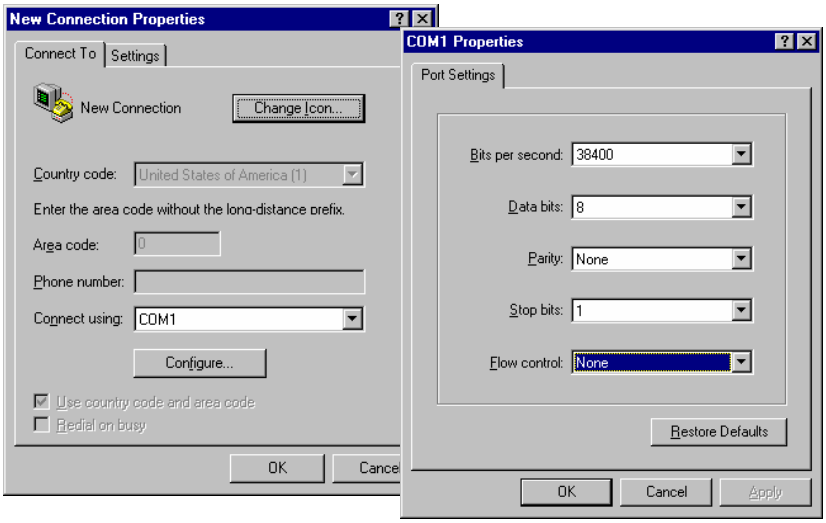


7. Configuring gateway through RS232 serial port

Gateway can be configured through serial connection, telnet and web browser. Console and telnet have the same user interface. Before connecting to network, users have to setup the IP address for Gateway through serial connection. MS Windows's HyperTerminal is a good choice to configure Gateway. The following settings are the values for serial terminal connection to Gateway.

- Speed: 38400 bps
- Data bits: 8
- Parity check: none
- Stop bit: 1
- Flow control: none





If the setting is as listed, Gateway will show the following menu in the Console/Telnet.

Notice:
There are two staged password login

- **The first stage login password is "VoIP" for only network setting**
- **The second stage login password is "antek" for fully gateway function setting.**

Login: antek

```
-----------------------------------------------------
----  antek VSP-5004(1B)  Version 1.1.1 (5409)  ----
-----------------------------------------------------
 1. Set WAN Port network parameters.
 2. Set H.323/SIP related functions.
 3. Set Port's Dialing Number.
 4. Set Hot Line Calls.
 5. Set Direct Dialing Numbers.
 6. Show All Numbering Plan.
 7. Voice processing Control.
 8. Gateway access Control.
 9. Advanced Configurations.
 a. Set to the Default Configurations.
 b. Voice calls Monitoring.
 c. Extended Configurations.
 d. BandWidth Control/Shaping.
 e. NAT Configurations.
 f. Save Current Configurations to Rom.
 g. Restart the System.
 h. Logout.
Key in 1 - h :
```

You may key in the selected item and press enter to process the command. For telnet users, you will get the prompt, please enter telnet password.

```
telnet 10.10.10.51
Login password:
```

User can change the default password under the "8. Gateway access Control":

Notice:

1. **The default Telnet IP address is "10.10.10.51".**
2. **The default Telnet password is "antek" or "VoIP".**
3. **Press Ctrl + 'a' will reset all setting values back to factory default.**

8. Set Network Parameters

The first thing you need to do is setting the ip address, please key in '1' and enter to set network parameters.

```
My IP = 10.10.10.51
Default Router IP = 10.10.10.254
Network Mask = 255.255.255.0
My MAC address = 0:4:f:11:11:22
CDR Server IP = 0.0.0.0

1. Change My IP address.
2. Change the Default Router IP address.
3. Change the Network Mask.
4. Enable DHCP Client.
5. Enable PPPoE Client.
6. Ping.
7. Pass Through NAT/Firewall
 8. Change CDR Server IP. (Set IP=0 will disable it.)

 'Esc' to Main Menu.
Choose one item :
```

You can set fixed IP or dynamic IP address by choosing PPPoE or DHCP methods, please contact your network administrator to know the settings about your network parameters.

Notice:

If you are using PPPoE to get dynamic IP address, the PPPoE will require username and password to connect to ISP.

In Taiwan, the given username should append @hinet.net (eg: 12345@hinet.net) as the username in the PPPoE username setting.

After above steps have been done:

- Press "Esc" for returning to main menu.
- Press 'f' to save current configurations to ROM.
- Then press "g" to restart the Gateway system.

If all the network settings are correct, Gateway will connect to the network.

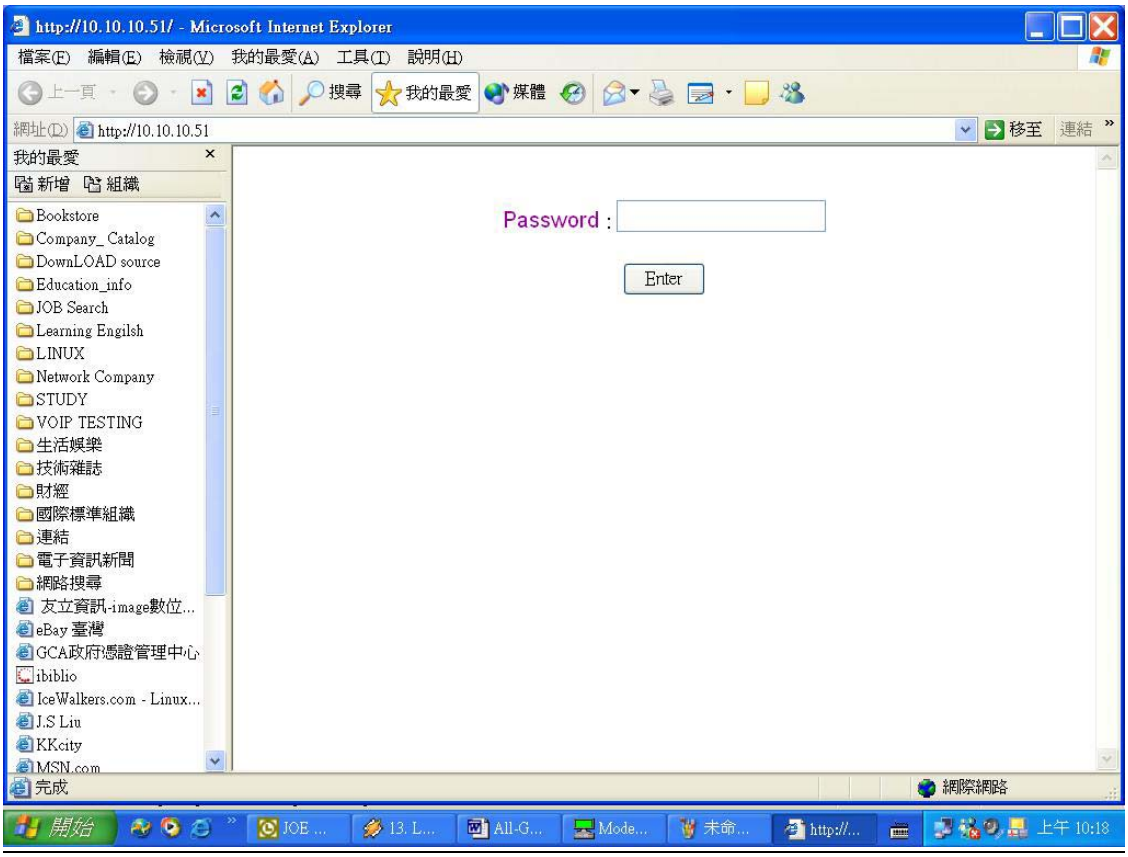
9. Using Web Browser To Configure Gateway System

9.1 Connecting to the gateway from web browser

When Gateway is connected to the network, you can easily configure the system by using web browser

Step:

- In the web browser, please key in the IP address (e.g. http://10.10.10.51) of the Gateway as URL, then the browser will connect to the Gateway and user can see the following web page:

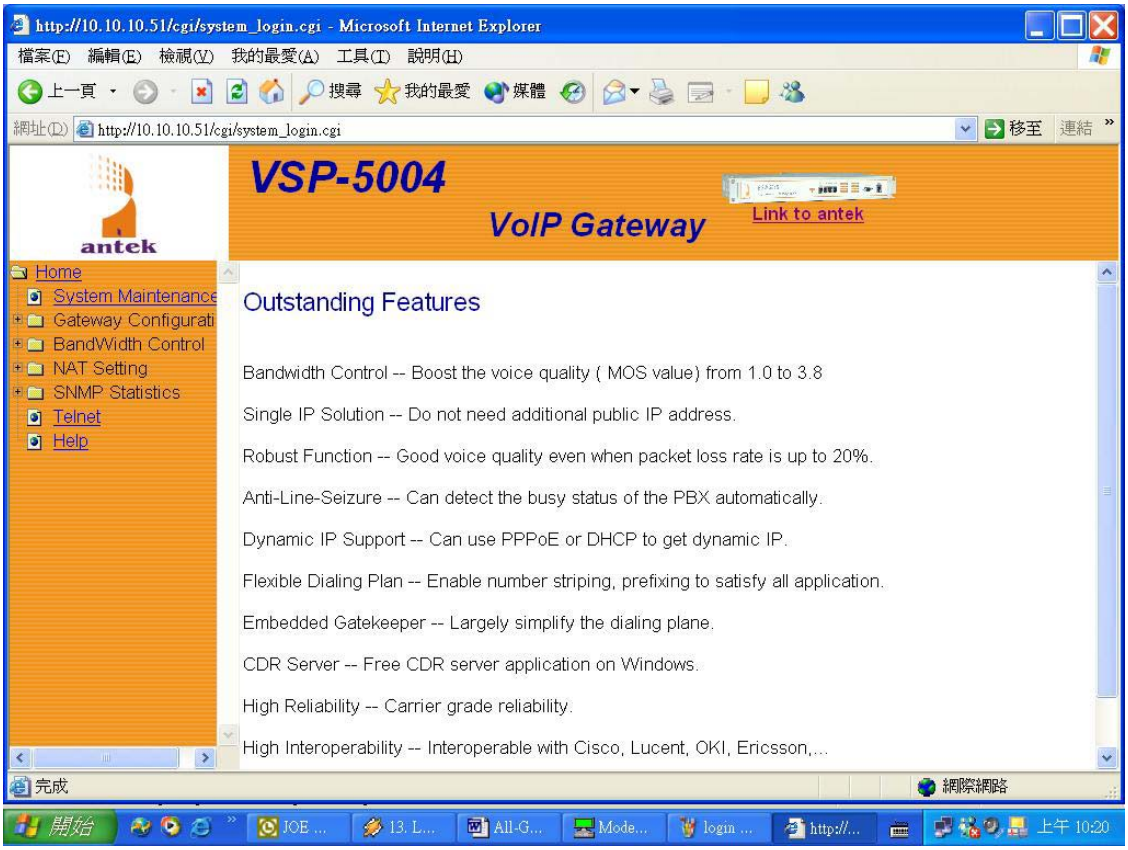


Notice:

1. **The default password for "View System Status" is "antek".**
2. **The default IP for Gateway is "10.10.10.51".**

9.2 Change configuration of the system

After you completed the login steps in 9.1, you will see the following page. Now you can change the system setting. The main menu is on the left side, and it includes three main categories “Gateway Configuration”, “Bandwidth Control” (VSP-Series) and “SNMP Statistics”. They will be explained in the following sections.

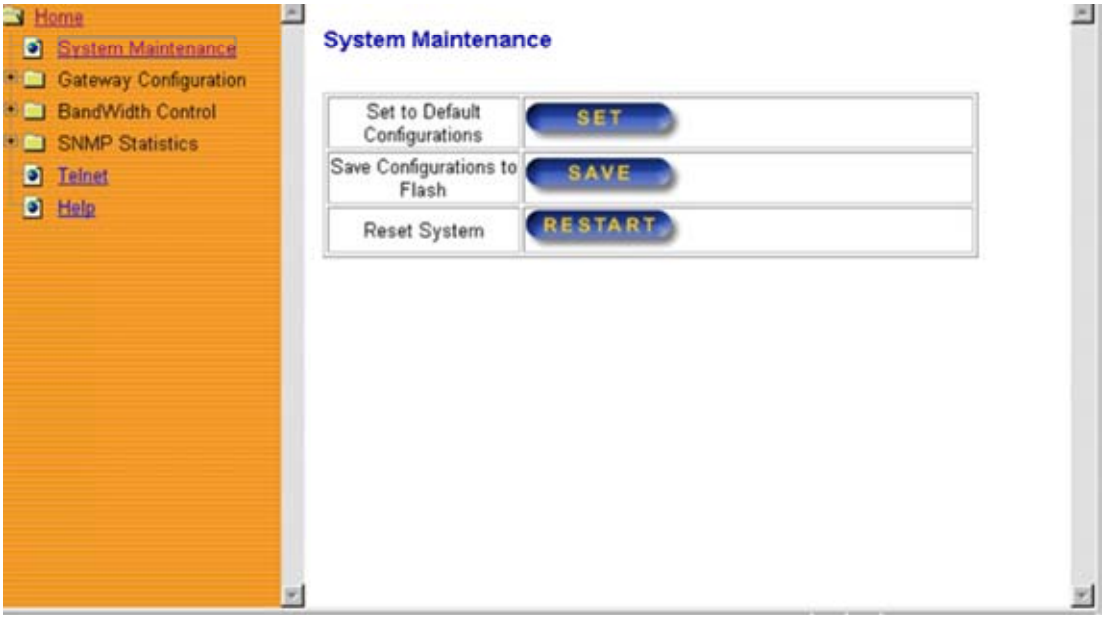

http://10.10.10.51/cgi/system_login.cgi - Microsoft Internet Explorer
http://10.10.10.51/cgi/system_login.cgi
VSP-5004
VoIP Gateway
Link to antek
Home
System Maintenance
Gateway Configurati
BandWidth Control
NAT Setting
SNMP Statistics
Telnet
Help
Outstanding Features
Bandwidth Control -- Boost the voice quality (MOS value) from 1.0 to 3.8
Single IP Solution -- Do not need additional public IP address.
Robust Function -- Good voice quality even when packet loss rate is up to 20%.
Anti-Line-Seizure -- Can detect the busy status of the PBX automatically.
Dynamic IP Support -- Can use PPPoE or DHCP to get dynamic IP.
Flexible Dialing Plan -- Enable number striping, prefixing to satisfy all application.
Embedded Gatekeeper -- Largely simplify the dialing plane.
CDR Server -- Free CDR server application on Windows.
High Reliability -- Carrier grade reliability.
High Interoperability -- Interoperable with Cisco, Lucent, OKI, Ericsson,...

Steps:

- Click on “System Maintenance” from the menu, and move to next page.

9.2.1 Gateway System Maintenance

In this page, you have 3 choices for setting the system to default configuration, saving current configuration or restarting the Gateway.



Steps:

- Press “SET” button can restore the settings to default values.
- Press “SAVE” button can write current settings to flash.
- Press “RESTART” button, the system will be restarted.

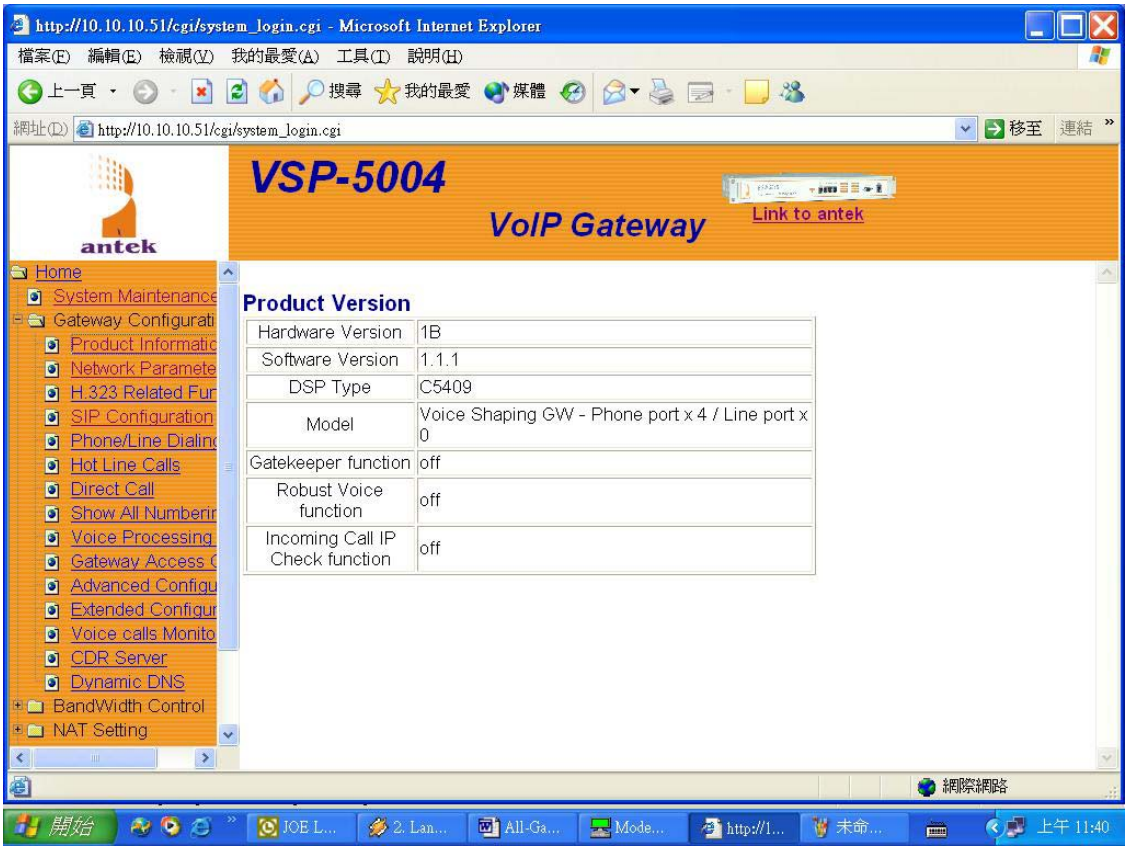
Notice:

1. **“Save” every time after you change settings, then “Restart” the system.**

9.3 Gateway Configuration

9.3.1 Product Version

After “Product Version“ is clicked under the “Gateway Configuration” menu, you will see the following page. In this page, you can find the information related to this Gateway product, including Hardware version, Software version, Model, DSP type, etc.



Steps:

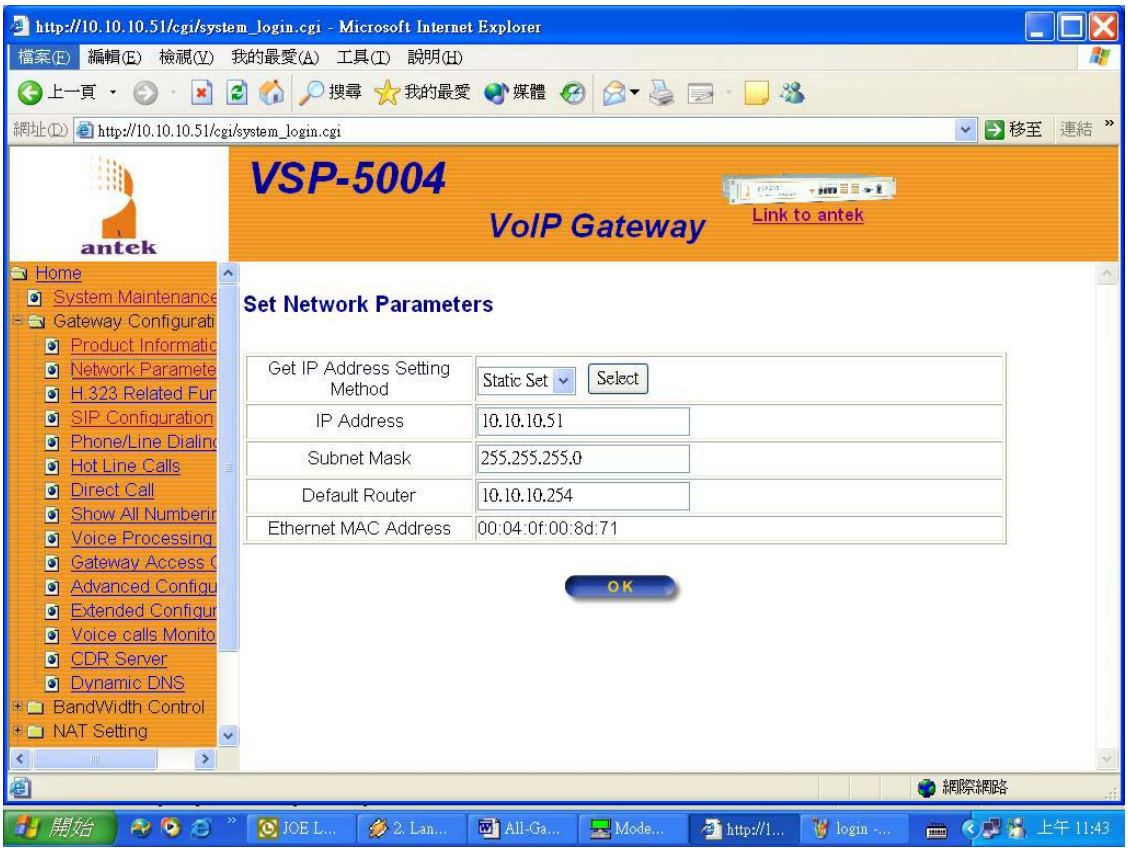
- Click “Product Version” under the “Gateway Configuration” menu.

9.3.2 Network Parameters

By clicking on “Network Parameters” under the “Gateway Configuration” menu, users can change network parameters.

Steps:

- Select from the combo box to choose the method for getting IP address, it can be “Static set”, “DHCP“ or “PPPoE“. Press “SET” button to confirm it.
- If “Static Set” is selected, key in IP address, subnet mask and default router to corresponding field. Press “OK” button to change these parameters.
- If “DHCP” is selected, the related network parameters will automatically get from the DHCP server.
- If “PPPoE” is selected, you need to fill in the username and password fields. In this setting, the network parameters are got from PPPoE server.
- For NAT function, the LAN port IP address is designed for LAN interface and only activated when the NAT function is turn on.
- Press “OK” button to confirm the setting. Notice that, if this setting is changed, you need to save and restart the system to make the work.



9.3.2.1 Settings for Console/Telnet only

1. Set the network parameters.
   - 1-6 Ping.
   - 1-7 Pass Through NAT/Firewall
     - 1-7-1 Enable Pass Through NAT/Firewall Function.
     - 1-7-2 Change Base Port.
     - 1-7-3 Select the Type of Public IP of NAT/Firewall.
     - 1-7-4 Set the Public IP of NAT/Firewall.

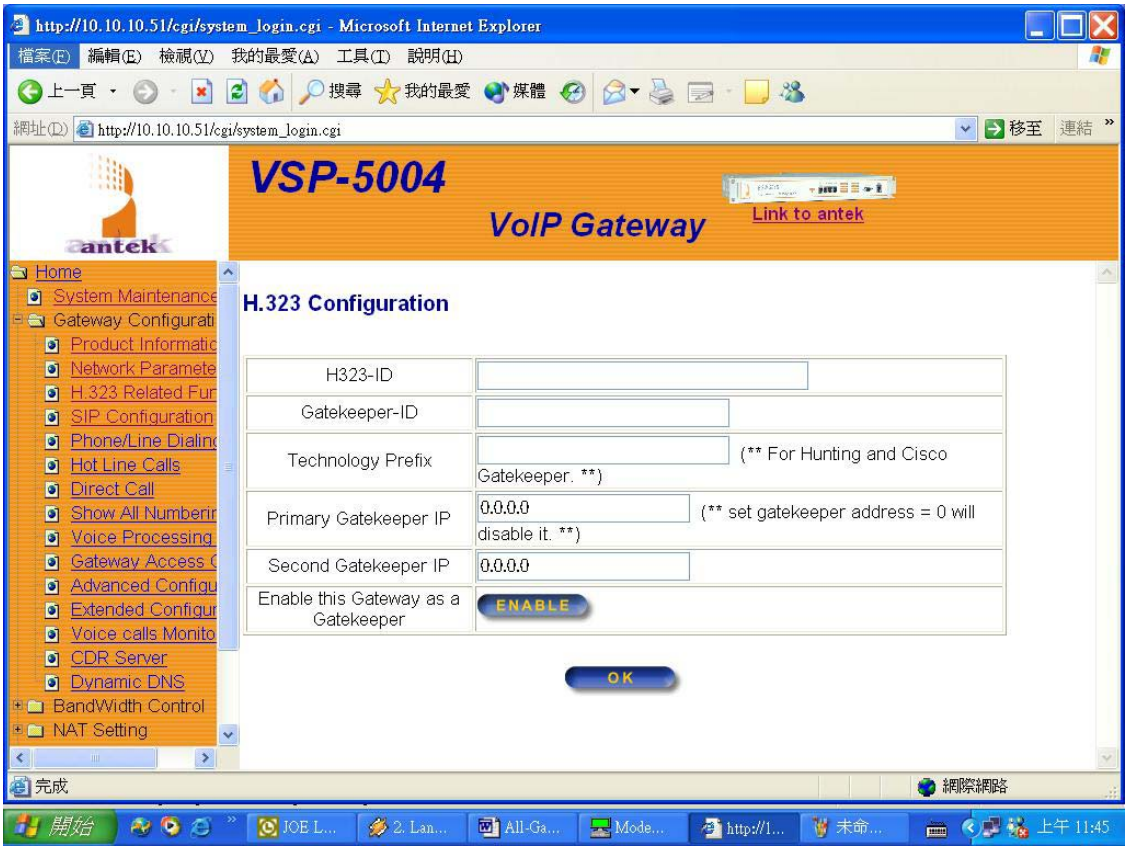
9.3.2.2 Passing-through NAT/Firewall

- Enable Pass Through NAT/Firewall Function
- Please set the Base Port, the gateway will use only those TCP/UDP ports range from Base Port to Base Port + 20, for example, if the Base Port is 1719, then only the ports 1719 to 1738 are used by all the VoIP TCP/UDP connections. In order to let the gateway passing through the NAT device, the NAT device must enable the "virtual server" function to map the port range from 1719~1738 to the gateway. Thus, any TCP/UDP connections within this port range (1719~1738) will connect to the gateway.
- Select the type of Public IP of NAT/Firewall, the type is fixed ip or dynamic ip. If the NAT device is using fixed ip address, then the gateway need to set this fixed public IP address. If the NAT device is using **dynamic ip address**, the gateway will need the help of the **CDR server software**. The CDR server software can tell the gateway the NAT device's dynamic IP address.
- If the NAT device is using dynamic ip address, the gateway must register to a gatekeeper to work properly.
- If there is only one gateway behind the NAT device and the NAT device is using a fixed ip address, you don't need the gatekeeper.
- Please be noticed that some kind of NAT device could try to do H.323 address translation, but doing not correctly, in this situation, the NAT pass-through function could fail.

Notice:

1. **You can use console/telnet to control the gateway and ping others if you would like to ping another device from the gateway.**
2. **Please go to menu 1-6 under the console/telnet to do so.**

9.3.3 H323 Configuration



Usage:

- The "H323-ID" is the H323-ID of this gateway when registering to the gatekeeper
- The "Gatekeeper-ID" is the gatekeeper's ID, usually do not need to set this field unless the gatekeeper must need this value.
- **Gatekeeper backup:** There are two gatekeeper address fields, one is primary, the other secondary. If this gateway does not want to register to any gatekeeper, just set value 0 to the primary gatekeeper address. If the primary gatekeeper address is not 0, the gateway will register to the primary gatekeeper. If the second gatekeeper is not 0, the gateway will try to register to the second gatekeeper when failed to register to primary gatekeeper, i.e. if both the primary gatekeeper and second gatekeeper addresses are present, the gateway will try to register to these two gatekeepers respectively. The gateway can have the gatekeeper backup function by this way.
- **Hunting function:** The "Technology prefix" is for hunting usage, when many gateways wanted to be hunted by a same number, you can assign the "Technology prefix" here to register this prefix number to the gatekeeper. The gatekeeper will hunt those gateways with the same prefix address alternatively and skip those gateways that have no available ports. The gateway must also assign the local

dialing plan in the “direct dial plan” field to tell this gateway how to handle the “prefix address”. For example, if the prefix address is 001, then there must be an element in the “direct dial plan”, suppose the dial plan is leading number = 001, destination = port 1,2,3. Then the gateway will report to the gatekeeper that this gateway has three available ports. Any time the available ports 1,2,3 are changes, the status will be reported to the gatekeeper. This hunting mechanism must co-work with the embedded gatekeeper.

- If the gateway is going to be used as a gatekeeper, just press “ENABLE” button to enable gatekeeper function on this gateway. (Gatekeeper models only). When this gateway is used as a gatekeeper, all the gateway functions are still the same.

9.3.3.1 Gatekeeper related functions

Gatekeeper backup functions:

- The gateway can assign both the primary gatekeeper and the secondary gatekeeper to enable the GK backup function.
- The gateway will try to find the next available GK, when the current GK has no response for 30 seconds.
- The gateway will switch between these two GK when the current GK has no response.

Technology Prefix: (For Hunting or Cisco Gatekeeper Usage)

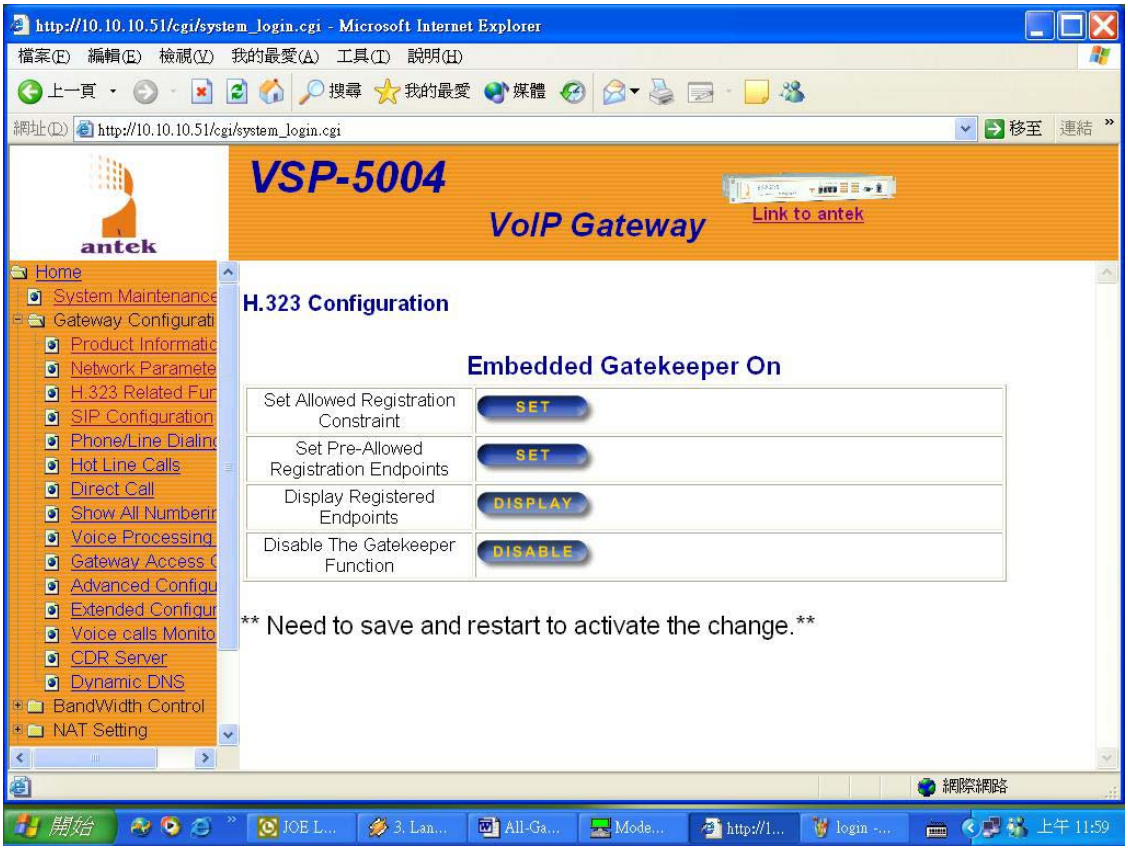
- Used by hunting or Cisco Gateway/Gatekeeper
- This prefix will register to gatekeeper. Examples: 001, 002, or 01#, 02#, 03# for Cisco gatekeeper.
- When this prefix is set, all other numbers will not register to gatekeeper.
- All gateways with the same prefix are hunted together.

Hunting function:

- The (Technology) prefix address if assigned, the hunting function of the gateway is enabled.
- All the gateways with the same prefix address are hunted cyclically.
- The hunting numbers must be added in the gateway (direct dialing number) to find the destination ports.
- The gateway will report current available ports to the GK when any port status is change.
- The GK will hunt cyclically unless one gateway has no available ports.

9.3.3.2 Embedded Gatekeeper On (for Gatekeeper model)

When the embedded gatekeeper function is on, the following page is shown as below.



9.3.3.2.1 Set Allowed Registration Constraint (for Gatekeeper model)

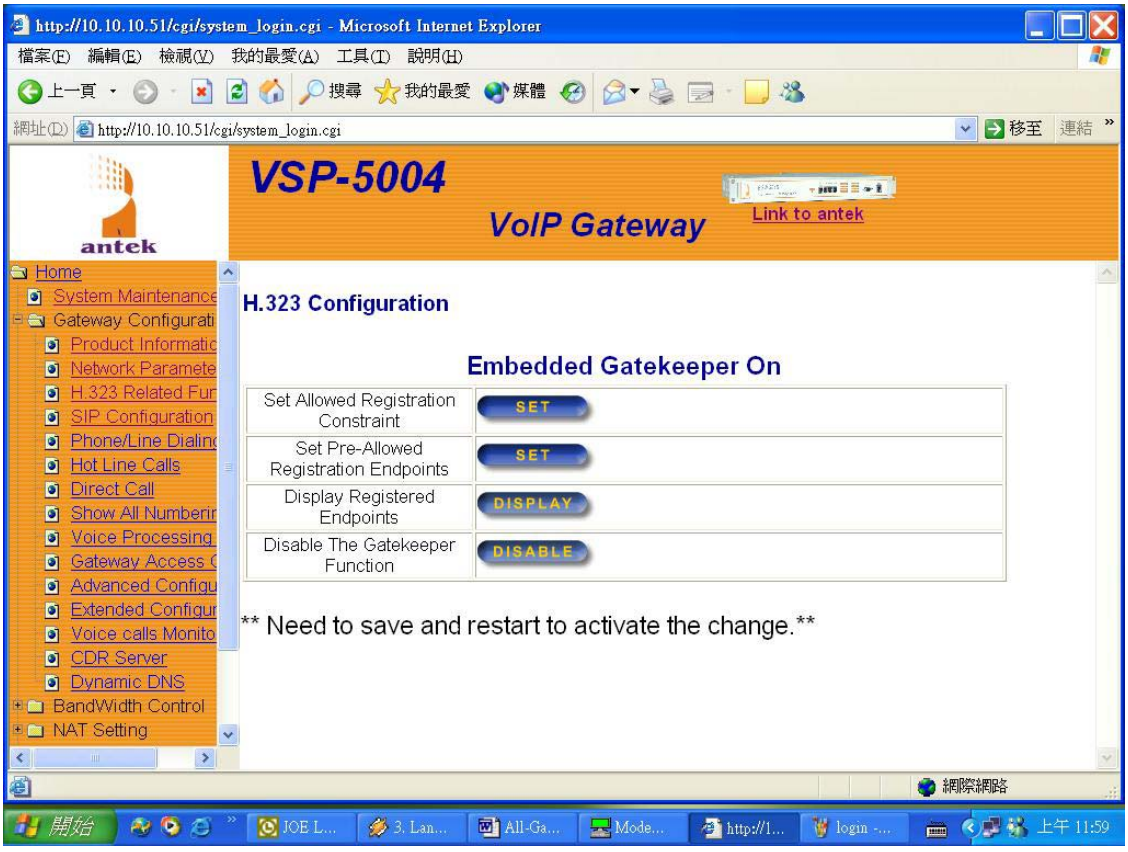
"Set Allowed Registration Constraint" is used to restrict other gateways to register to this embedded gatekeeper. If this function is not enabled, any other gateway can register to this embedded gatekeeper.

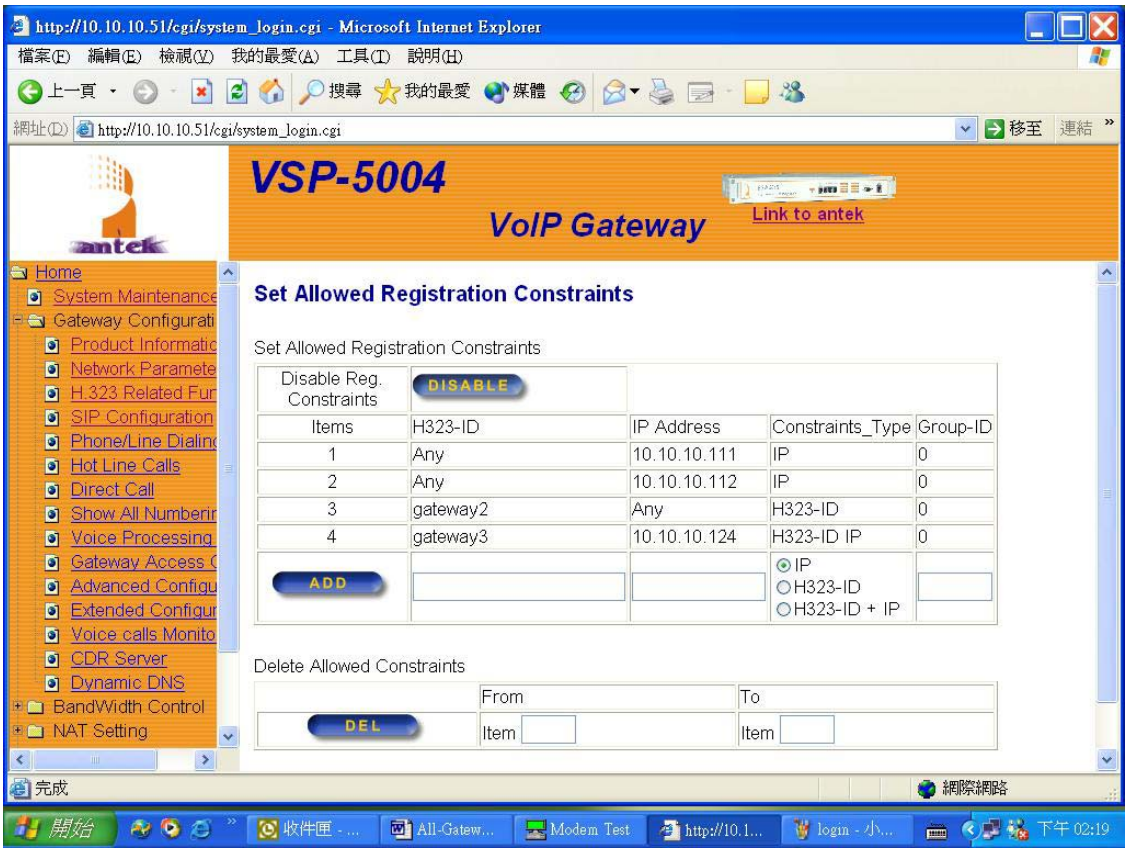
Steps:

- Pressing "SET" button in "Set Allowed Registration Constraint", the following page is displayed.
- Press "ENABLE" button to enable this function.

Notice:

- If the "ENABLE" button is pressed, only those H323-ID or IP address in the constraint table are allowed to register to this embedded gatekeeper. If the constraint table is empty, no gateway is allowed to register in.





Usage:

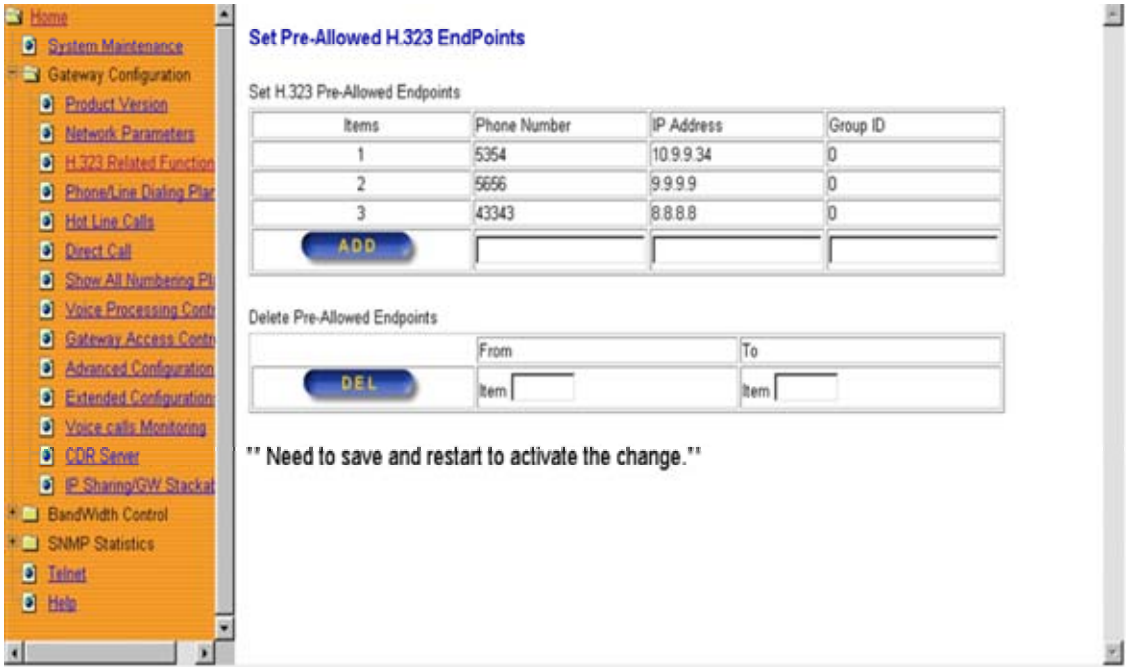
- Select from radio box to choose the method of registration constraints, the constraint could be H-323 ID or IP Address or both (IP address + H.323 ID).
- Input H323-ID, IP address or both according to your selection.
- Press “ADD” button to add it.
- For delete function, input the start and stop item number you want to delete. Press “DEL” button to delete them.
- Press “DISABLE” button if you want to disable the registration constraint function.
- **Group function:** there is a “**Group ID**” field in the last of the constraint table, you can specify different “group id” to different entries if you want to do the grouping function, those gateways with the same group id will belong to the same group, only those gateways in the same group can talk to each other. The gatekeeper itself is default to **Group ID = 0**. All the dialing plan or registered numbers in one group are independent with those dialing plan or registered numbers in other group, i.e. different gateways in different groups could have the same numbers registering to the gatekeeper. You can specify all the gateways to the group id = 0 if the grouping function is not to be enabled.

9.3.3.2.2 Set Pre-Allowed Registration Endpoints (for Gatekeeper model)

The "Set Pre-Allowed Registration Endpoint" function can let other gateways/endpoints that do/can not register to this embedded gatekeeper have the ability to make calls to any gateways/endpoints that are registered to the embedded gatekeeper.

Steps:

- By pressing "SET" button in "Set Pre-Allowed Registration Endpoint", the following page is displayed.
- Specify the phone number and IP address of those pre-allowed gateways/endpoints in the "Set H.323 Pre-Allowed Endpoints" table.
- Press "ADD" button to add it.
- If you want to delete any items, input the start and stop item number you want to delete. Press "DEL" button to delete them.
- **Group function:** there is a "group id" field in the last of the "pre-allowed" table, you can specify different "group id" to different entries if you want to do the grouping function, those pre-allowed gateways with the same group id will belong to the same group, only those gateways in the same group can talk to each other(and to those registered gateways with the same group id). The gatekeeper itself is default to group id = 0. All the dialing plan or registered numbers in one group are independent with those dialing plan or registered numbers in other group, i.e. different gateways in different groups could have the same numbers registering to the gatekeeper. You can specify all the gateways to the group id = 0 if the grouping function is not to be enabled.



Notice:

- **When a gateway's number is set in the "pre-allowed" table, this gateway is considered "registered" to the gatekeeper, i.e. the following two functions will be available:**
  1. **The gateway can make calls to any other gateways that have registered to the gatekeeper. (But the dialing plan must be set in the pre-allowed gateway itself.)**
  2. **Any registered gateways can make calls to the pre-allowed gateway.**

GK group function usage:

- If the "Set allowed registration constraint" is enabled, the grouping function is enabled. Each registration constraint has an additional "group_id" field to assign the belonged group (from 0 to 31).
- If the grouping function is enabled, all gateways must be in the "registration constraint" for assigning to their belonged group.
- The gatekeeper it self is default to group 0.
- Each group cannot talk to another group.
- The "Preallowed gateway/endpoints" table also can assign each predefined group id.

GK grouping function specification:

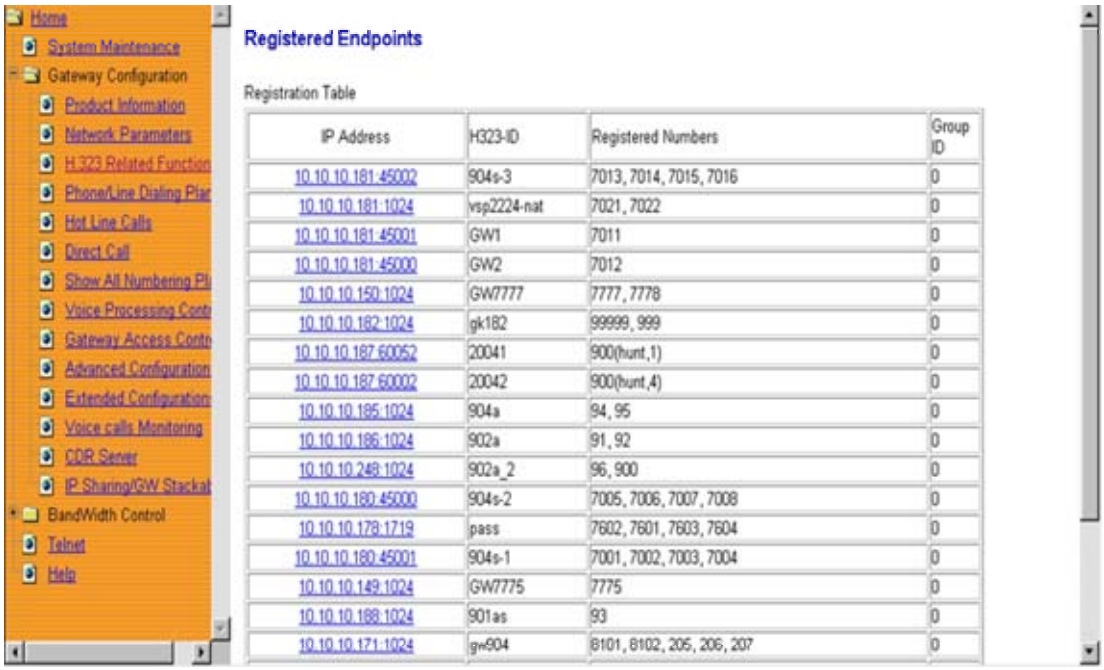
- Can have 32 registration groups (0~31). Each group can have its own dialing plan.
- Each group can allow 200 gateways to register, but totally (including all groups) can allow 200 gateways to register.
- Each gateway can register up to 32 numbers.
- Maximum totally registered numbers is 2048 (including all registered numbers in all groups).

9.3.3.2.3 Display Registered Endpoints (for Gatekeeper Model)

This selection will display all the registered gateways/endpoints. The displayed information includes IP address, H323-ID and the registered aliases (phone numbers).

Steps:

- Press "DISPLAY" button shown in 9.3.3, the following page is displayed.
- By clicking on the "**IP address**" of the registered gateway, a new web page will be opened displaying the home page of that registered gateway.
- If there is a **(hunt, n)** appeared in the "registered number" field, it means that the registered number is for hunting usage, the number n is currently available port number of the gateway.

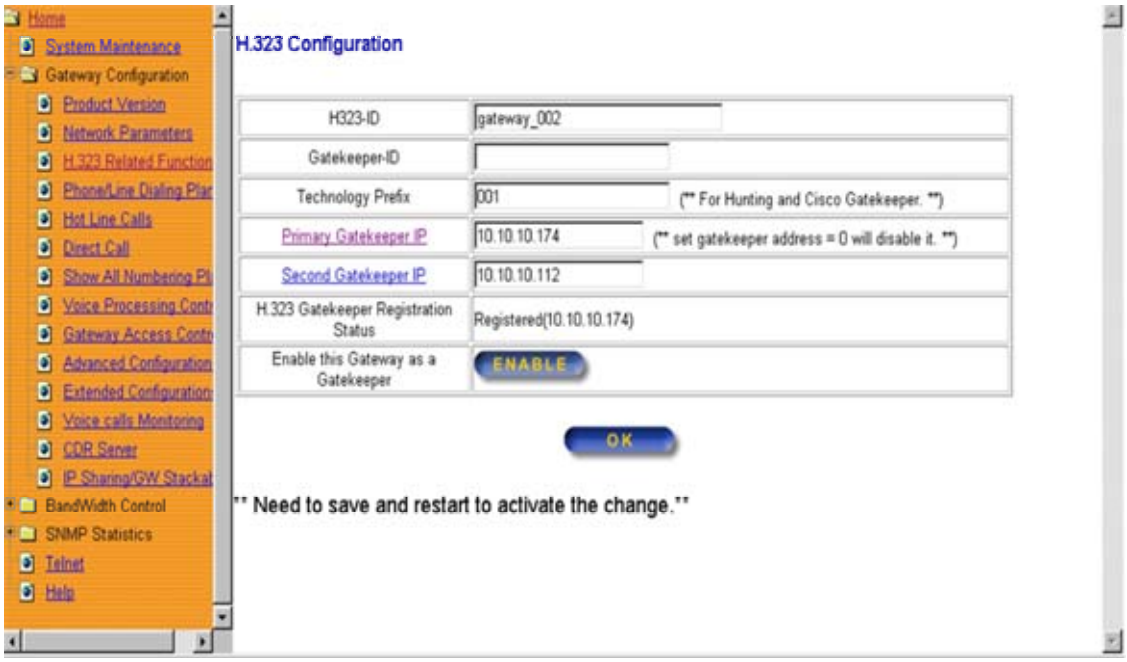

Home
System Maintenance
Gateway Configuration
Product Information
Network Parameters
H.323 Related Function
Phone/Line Dialing Plan
Hot Line Calls
Direct Call
Show All Numbering Plan
Voice Processing Control
Gateway Access Control
Advanced Configuration
Extended Configuration
Voice calls Monitoring
CDR Server
IP Sharing/GW Stacking
BandWidth Control
Telnet
Help
Registered Endpoints
Registration Table
IP Address
H323-ID
Registered Numbers
Group ID
10.10.10.181:45002 904s-3 7013, 7014, 7015, 7016 0
10.10.10.181:1024 vsp2224-nat 7021, 7022 0
10.10.10.181:45001 GW1 7011 0
10.10.10.181:45000 GW2 7012 0
10.10.10.150:1024 GW7777 7777, 7778 0
10.10.10.182:1024 gk182 99999, 999 0
10.10.10.187:60052 20041 900(hunt,1) 0
10.10.10.187:60002 20042 900(hunt,4) 0
10.10.10.185:1024 904a 94, 95 0
10.10.10.186:1024 902a 91, 92 0
10.10.10.249:1024 902a_2 96, 900 0
10.10.10.180:45000 904s-2 7005, 7006, 7007, 7008 0
10.10.10.178:1719 pass 7602, 7601, 7603, 7604 0
10.10.10.180:45001 904s-1 7001, 7002, 7003, 7004 0
10.10.10.149:1024 GW7775 7775 0
10.10.10.188:1024 901as 93 0
10.10.10.171:1024 gw904 8101, 8102, 205, 206, 207 0

9.3.3.2.4 Disable The Gatekeeper Function (for Gatekeeper model)

This setting is used to disable the embedded gatekeeper function in the Gateway system.

Steps:

- Press “DISABLE” button shown in 9.3.3, the following page is displayed.
- The embedded Gatekeeper function is disabled now.


Home
System Maintenance
Gateway Configuration
Product Version
Network Parameters
H.323 Related Function
Phone/Line Dialing Plan
Hot Line Calls
Direct Call
Show All Numbering Pl
Voice Processing Contr
Gateway Access Contr
Advanced Configuration
Extended Configuration
Voice calls Monitoring
CDR Server
IP Sharing/GW Stackat
BandWidth Control
SNMP Statistics
Telnet
Help
H.323 Configuration
H323-ID
gateway_002
Gatekeeper-ID
Technology Prefix
001
(** For Hunting and Cisco Gatekeeper. **)
Primary Gatekeeper IP
10.10.10.174
(** set gatekeeper address = 0 will disable it. **)
Second Gatekeeper IP
10.10.10.112
H.323 Gatekeeper Registration Status
Registered(10.10.10.174)
Enable this Gateway as a Gatekeeper
ENABLE
OK
** Need to save and restart to activate the change.**

9.3.4 SIP Usage Guide (Setting for Console/Telnet)

2. Set H.323/SIP related functions.
   2-1 Select Default VoIP protocol - 1.H323, 2.SIP : 2

```
------------------------------------------------------------------------------
                Use VoIP Protocol  = SIP
                Proxy Server is : None.
                Proxy Server Registering Period = 360 sec.

------------------------------------------------------------------------------

1. Set Default VoIP protocol.
2. Set SIP proxy server.
3. Set Registering Period.

'ESC' to Upper Menu
Choose one item( 1 - 3 ) :
```

There are two parts in the menu selections needed to be set for the SIP protocol usage.

9.3.4.1 SIP Configuration

Select main menu selection “2. Set H.323/SIP related functions.”, and then select submenu item “1”. Select Default VoIP protocol - 1.H323, 2.SIP. to select “2” the SIP protocol configuration, the configuration display is :

```
------------------------------------------------------------------------------
                Use VoIP Protocol  = SIP
                Proxy Server is: None.
                Proxy Server Registering Period = 360 sec.

------------------------------------------------------------------------------

 1. Set Default VoIP protocol.
 2. Set SIP proxy server
 3. Set Registering Period.
 'Esc' to Upper Menu.
 Choose one item (1-4) :
```

The first menu item is to select the “Default VoIP protocol”. This selection will define the VoIP signaling protocol used for all outgoing calls. If the “default VoIP protocol” selected is H.323, then all the outgoing call will use H.323 protocol to call out. If the

“default VoIP protocol” selected is SIP, then all the outgoing call will use SIP protocol to call out. But if any number is defined in “direct dialing plan”, that specific number will use it’s defined protocol.

The “2. Set SIP proxy server.” selection is to set the IP address/port of the proxy server. When this proxy server is set, the gateway will try to register to the proxy server no matter what’s the selection of “Default VoIP protocol”.(This situation is also true for H.323 registering, i.e. if the H.323 gatekeeper is defined, this gateway will register to the specific gatekeeper even if the “Default VoIP protocol” selected is SIP).

The “3. Set Registering Period.” is to set the interval that the gateway will re-register to the proxy server when previous registering is successful. If the registering is failed, the gateway will re-register every 10 seconds.

9.3.4.2 Direct dialing plan for SIP

If the “Default VoIP protocol” selected is the SIP protocol, all the outgoing VoIP calls will go to the proxy server using SIP protocols except some specific numbers defined in the direct dialing plan.

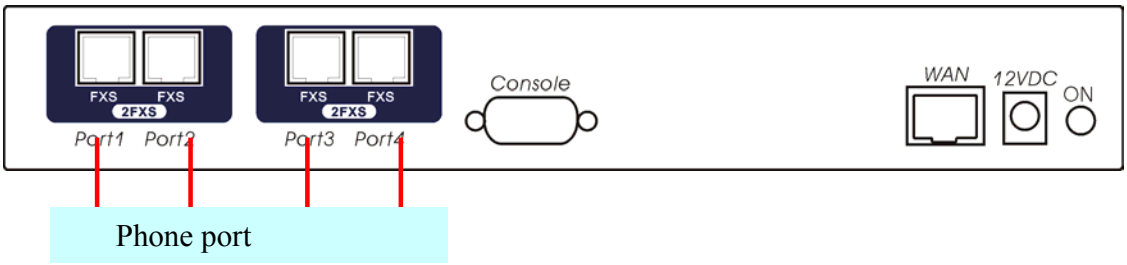
The gateway can set direct dialing plan for outgoing SIP calls no matter what’s the “default VoIP protocol”. This could be done by select “5. Set Direct Dialing Numbers.” in the main menu. When adding a new plan to the direct dialing plan, after key in all the necessary numbers, then select “Choose Destination - 1: Tel Port, 2: IP address: 3. Domain name to complete dial plan setting.

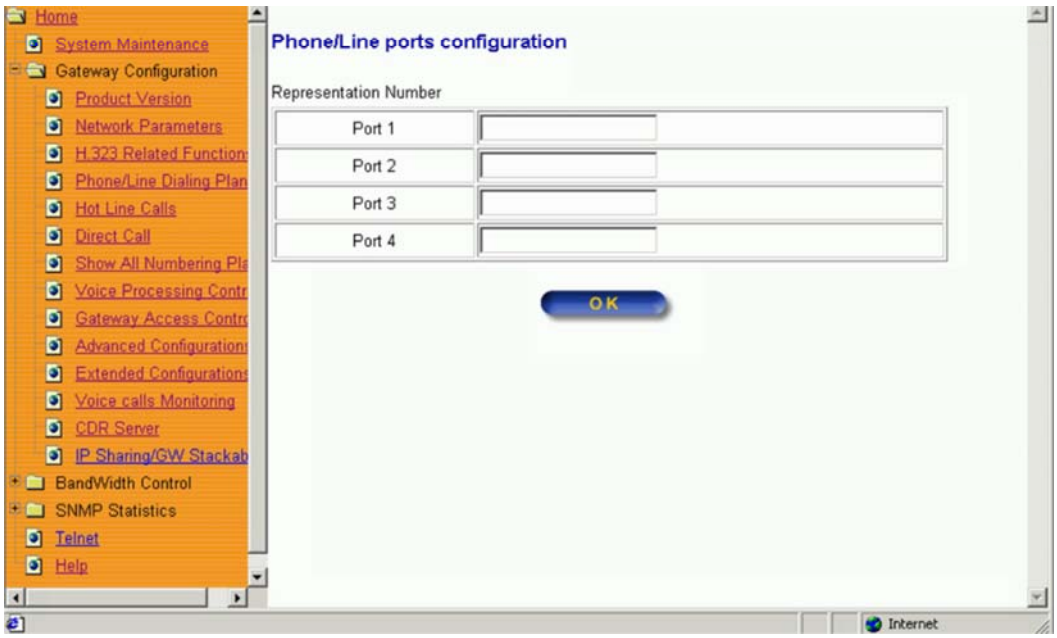
9.3.5 Phone/Line Dialing Plan

This section is describing the dialing plan of the gateway. Since there are many different gateways, the dialing plan could be divided into the following three major groups.

9.3.5.1 Phone Dialing Plan (EGW-802S, EGW-804S, VSP-5002S/5004S, VSP2500)

This configuration page is used to configure the numbering plan for those VoIP gateways with phone ports only.





9.3.5.1.1 Representation Number

Phone Number:

The representation number is the phone number of the telephone that is connected to Phone port.

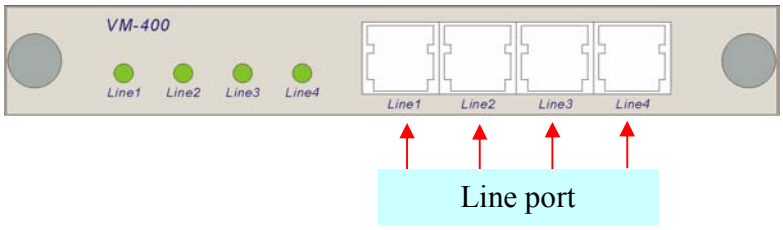
9.3.5.2 Phone/Line Dialing Plan (VSP-2500 only)

This configuration page is used to configure the numbering plan of the VSP-2500 Gateway. There are three different module models available for VSP-2500.

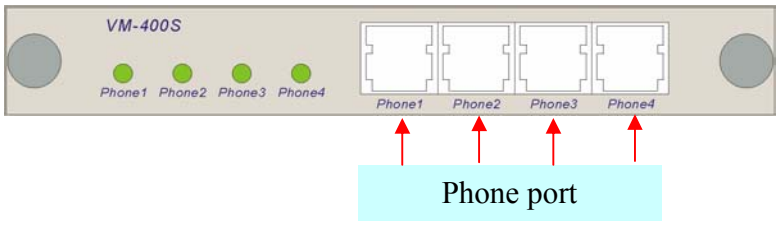
(Note: FXO port is connected to the extension port of a PBX or directly connected to a PSTN line)

VSP-2500 has 4 module slots. User can connect all 3 different kinds of module board into the VSP-2500 in any order or any slot.

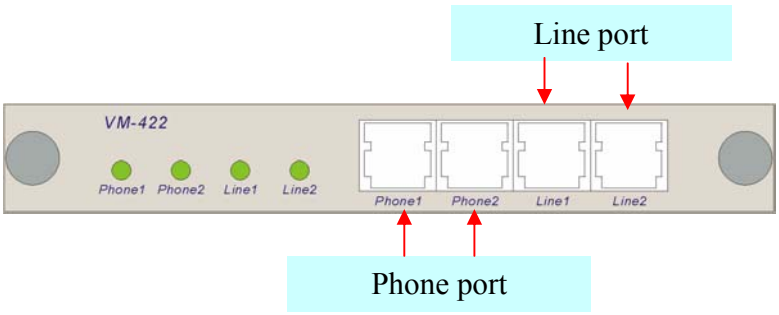
VM-402: 4 FXO ports module



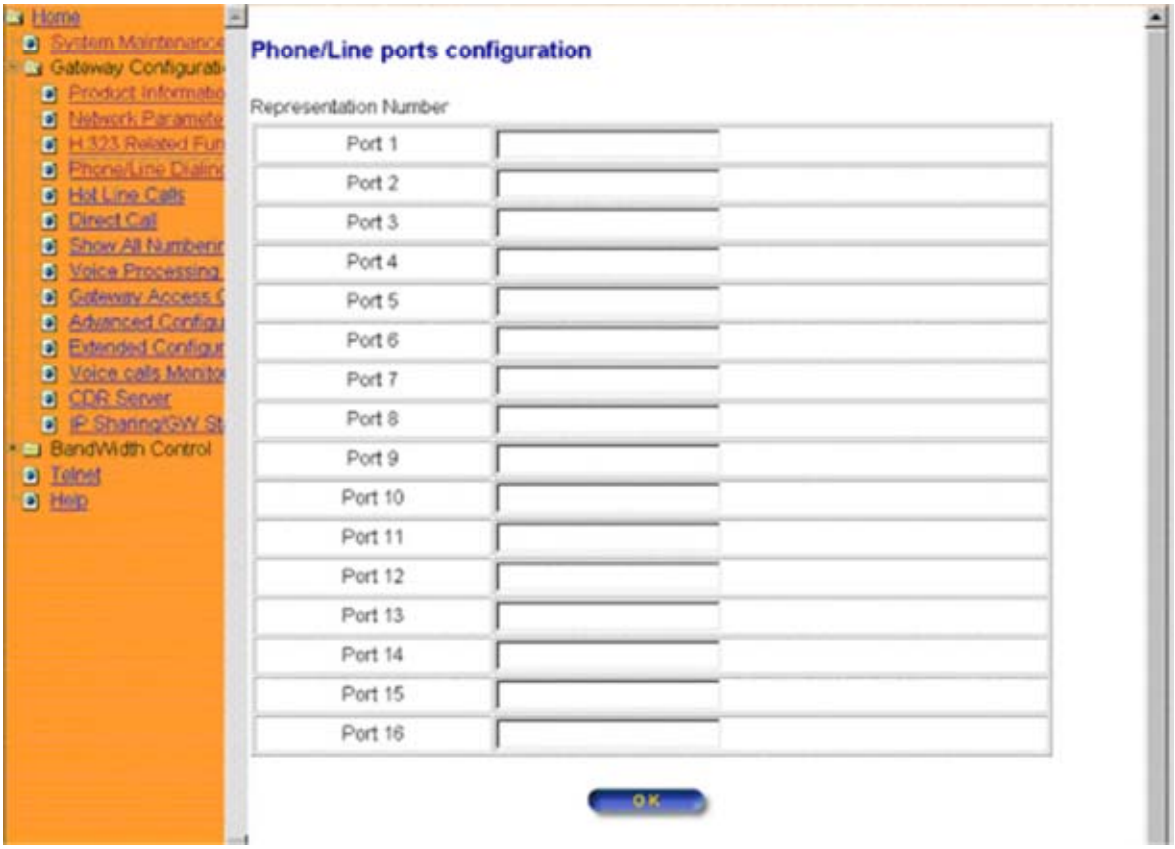
VM-401S: 4 FXS ports module



VM-442S: 2 FXO + 2 FXS ports module



The following page will be displayed when the "Phone/Line Dialing Plan" menu is selected.
The settings of the numbering plan are explained as the following:



Steps:

- Click “Phone/Line Dialing Plan” in left-side menu.

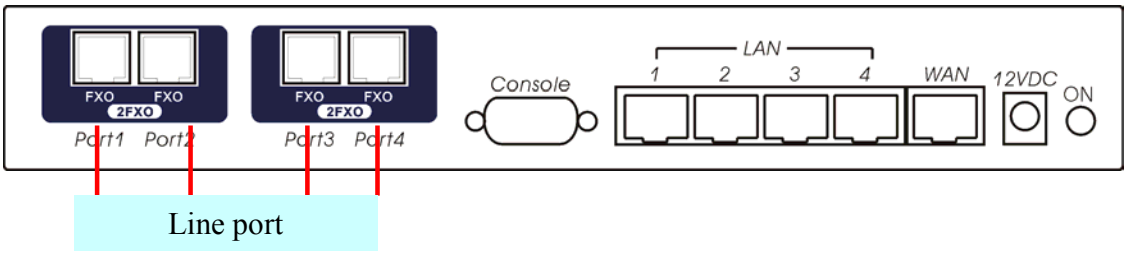
9.3.5.2.1 Representation Number

Phone Number:

The representation number is the phone number of the telephone that is connected to Phone port.

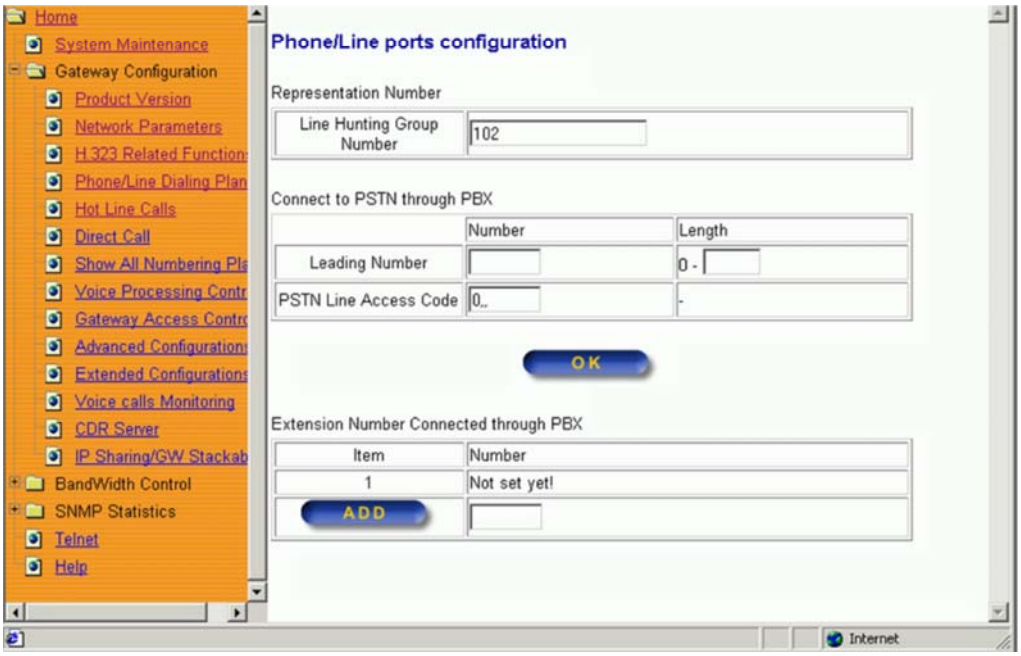
9.3.5.3 Phone/Line Dialing Plan (EGW-802, EGW-804, VSP-5002/5004, WRG-5002/5004 gateways with line ports)

This configuration page is used to configure the numbering plan of the VoiceShaper. There are 4FXO/4FXS/3FXO+1FXS/2FXO+2FXS/2FXS/1FXO+1FXS/1FXS different ports with VoiceShaper.



(Note: FXO port is connected to the extension port of a PBX or directly connected to a PSTN line)

The following page will be displayed when the "Phone/Line Dialing Plan" menu is selected.
The settings of the numbering plan are explained as the following:



Steps:

- Click "Phone/Line Dialing Plan" in left-side menu.

9.3.5.3.1 Representation Number

Phone Number:

The representation number is the phone number of the telephone that is connected to Phone port.

Line Hunting Group Number:

Line ports are connected to the extension ports of the PBX system or the PSTN line. They have a common Line Hunting Group Number. When this number is dialed, the Gateway system will find a free FXO line connected to PBX. This hunting will skip all busy lines and absent lines and find only the idle line to the PBX. After the available line is found, you can hear the dial tone from PBX. After that, you can dial the needed phone number out through PBX.

9.3.5.3.2 Connect to PSTN through PBX

The purpose of this setting is to set the one-step dial number to access to PSTN calls through PBX.

Representation Number:

When you want to dial to PSTN, this number is needed to identify this condition. Length is the min/max number of digits you can dial. The minimal length is 2.

Number to Access PSTN through PBX:

This is the external line access digit/number (usually‘0’) of the connected PBX.
After the previous “representation number” is dialed, the available line will be hunted first, then this access digit/number is dialed to the PBX to access the external line. Lastly, the real PSTN number will be dialed by the gateway to call through the PSTN.

9.3.5.3.3 Extension Number Connected through PBX

The purpose of these settings is to set the one-step dial number to access to the PBX’s extensions directly.
The extension numbers of the PBX can be added to this “extension table”. Any extension number when added to this table, it can be dialed from other gateway by simply calling this one-step number. Calls from other gateways will first be connected to this gateway; the gateway will then dial this extension into the PBX to ring the extension phone. This setting will largely simplify the dialing procedure of calling extensions.
You can use wildcard ‘x’ to resent a group of extension numbers. For example, 21x will include 210 to 219.

9.3.5.3.4 Delete Extension

This selection is used to delete the existing extension numbers.

Summary:

The following steps could summarize the whole settings of this “phone/line dialing plan” section:

Steps:

- Input the “Phone Number” and “Line Hunting Group Number” for FXS port and FXO port respectively.
- If the FXO port can access to PSTN, Input the number for “Representation Number” and its max. length, then input the number for “Number to Access PSTN through PBX”.
- Press “OK” button to change this setting.
- If needed, add extension number to the system, “x” represents the wildcard.
- Press “ADD” button will add one extension number.
- To delete the extension number, key in the start and end of the item to be deleted. Then, press “DELETE” button.

9.3.5.3.5 Settings for Console/Telnet only

3. Set Line Port Dialing Plan.

3-2 Set Line Port Connected PBX Extension Number

3-2-1 Add extension Numbers.
3-2-2 Delete extension Numbers.
3-2-3 Change extension Numbers.

.

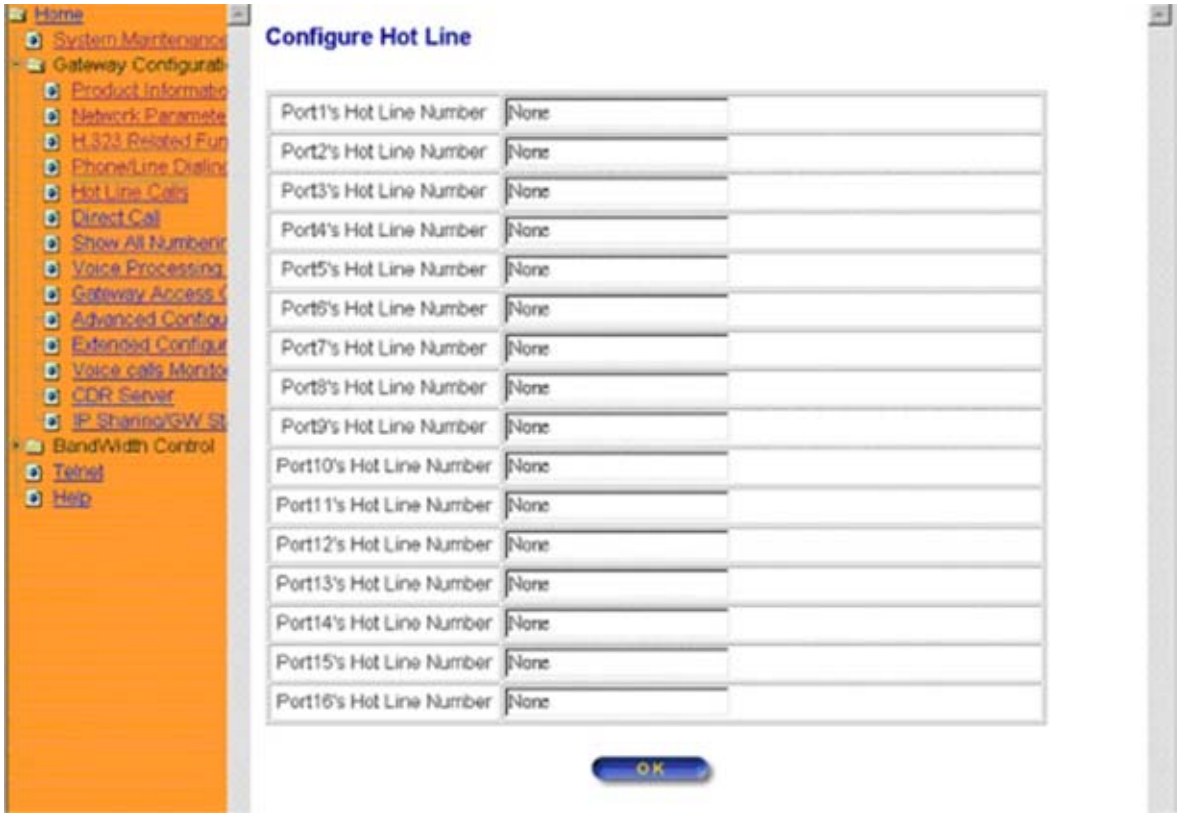
9.3.6 Hot Line Calls

The purpose of the “Hot Line Calls” setting is to let user do a “dial free” call. The configuration page is shown below:
If any hot line number is configured for a port, when the port-connected telephone is off hooked, the pre-configured hot line number will be automatically dialed out. This port cannot make phone call to any other number if its “hot line” number is set.

VSP-5004

Steps:

- Input hot line number for port 1 to port 4 respectively.
- Press “OK” button to save this setting.



VSP-2500

Steps:

- Input hot line number for port 1 to port 16 respectively.
- Press “OK” button to save this setting.

9.3.6.1 Settings for Console/Telnet only

4. Set Hot Line Calls.

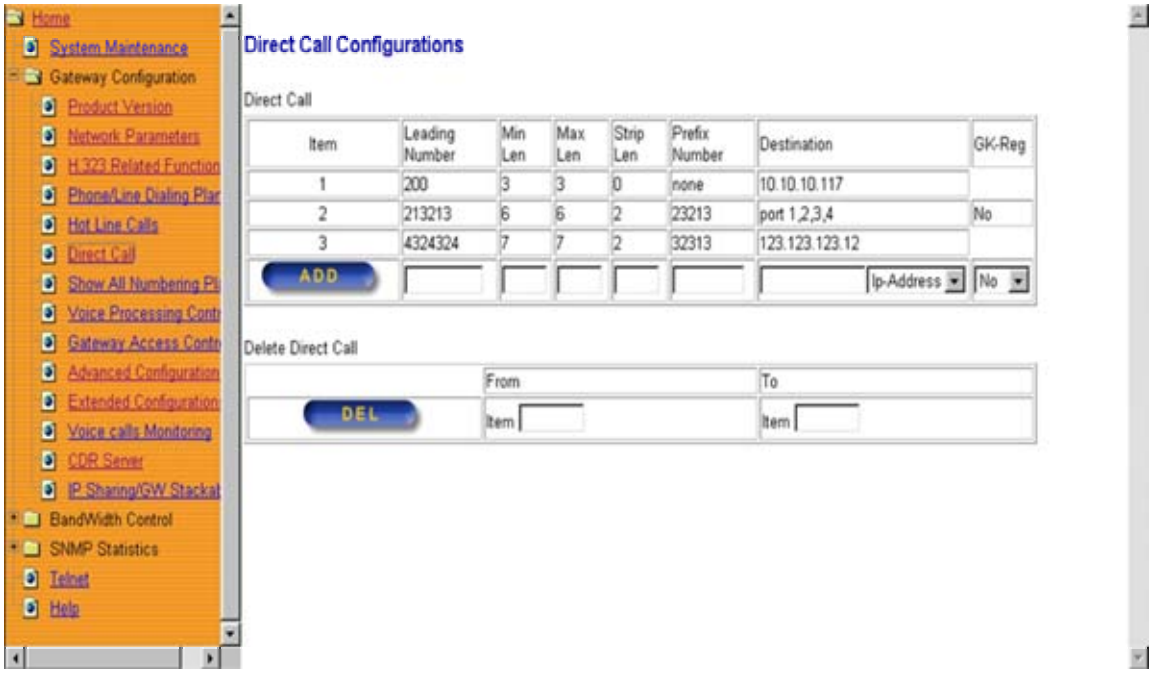
4-5.**Default Number of Empty call** is:

Some times, an incoming call from network could carry no called party number (no destination number, empty number), in this situation, the gateway could give this call a default number to be used as the called party number. This default number should be a port’s number, and then the phone set that connects to the specified port will ring.

9.3.7 Direct Call

The purpose of "Direct Call" setting is to let user create a proprietary dialing plan when this Gateway is not registered to any gatekeeper. This setting can also assign some dialing plan to local ports (including prefix strip, prefix addition).
Through this setting, user can directly map a number to a specific gateway (IP address).

- In the "Direct Call Configurations" settings:
  - "Leading Number" is the leading digits of the dialing number.
  - "Min Length" and "Max Length" is the min/max allowed length you can dial.
  - "Strip Length" is the number of digits that will be stripped from beginning of the dialed number.
  - "Prefix Number" is the digits that will be added to the beginning of the dialed number.
  - "Destination" is the IP address of the destination Gateway that owns this phone number. If the "Destination" is "Tel-port", this is for local dial plan setting.
  - **"GK-Reg**" can let user decides if this dialing plan will be registered to the gatekeeper or not when the destination is "Tel-port". This field could give the gateway more flexibility. If you want other gateways to call to this gateway, you must set "yes" value in the "GK-Reg" field.

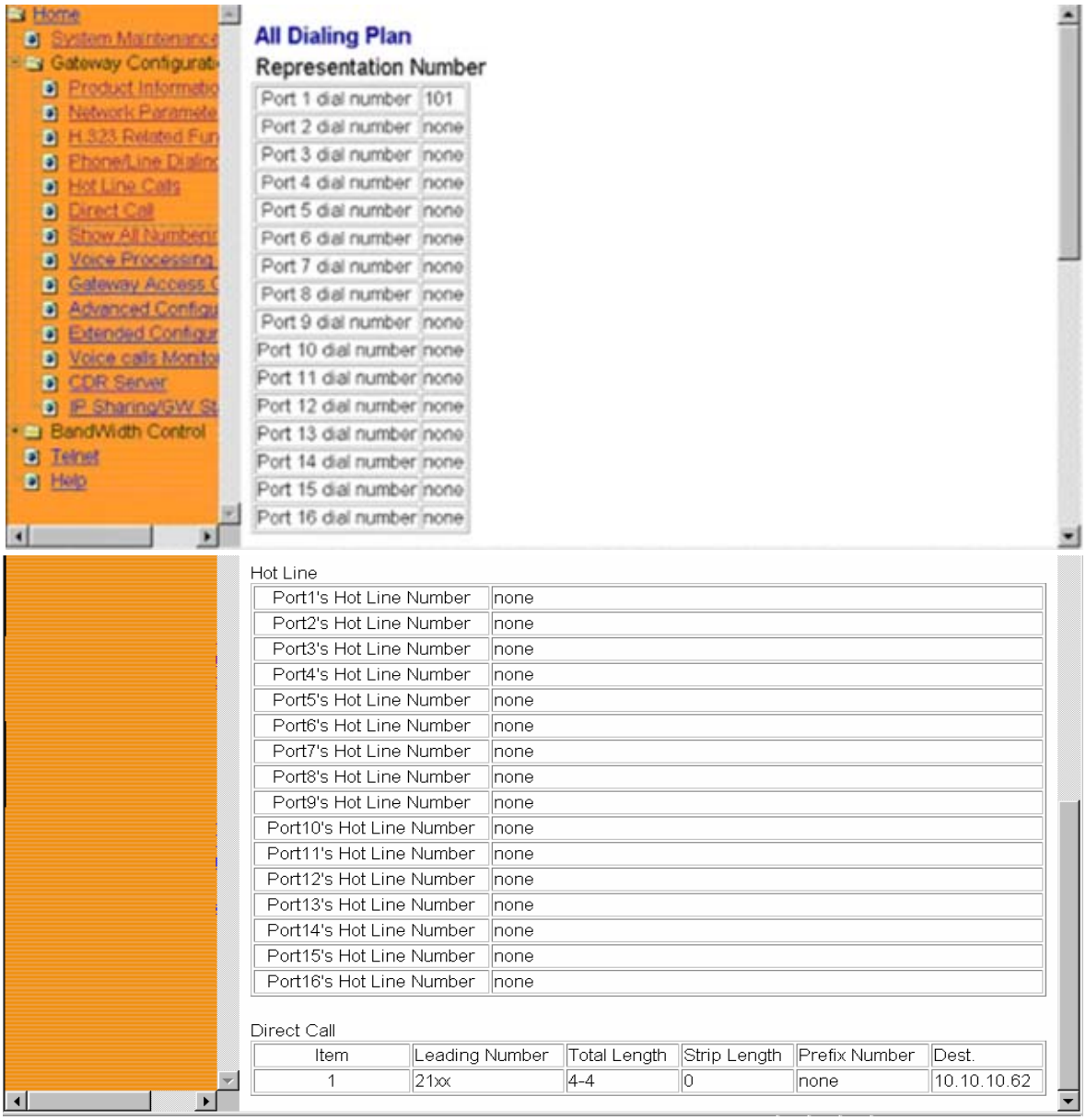


Steps:

- If you want to add a direct call item, fill all the blank fields of “Direct Call” table.
- Select form combo box to choose “Tel-port” or “IP Address”.
- If “Tel-port” is chose, this direct call is out through local analog port(local dial plan).
- If “Tel-port” is chose, you can also set “yes” or “no” in the “**GK-Reg**” field to decide if the “leading number” will register to the gatekeeper or not.
- If “IP Address” is selected, this direct call number is out through network.
  Notice: this setting is effective only when this Gateway is not registering to another gatekeeper.
- Press “OK” button to add an item.
- If you want to delete a direct call item, input the items you want to delete. Press “DEL” button to delete it.

9.3.8 Show All Numbering Plan

All the numbering plan of this Gateway system will be shown by this selection, as displayed below:

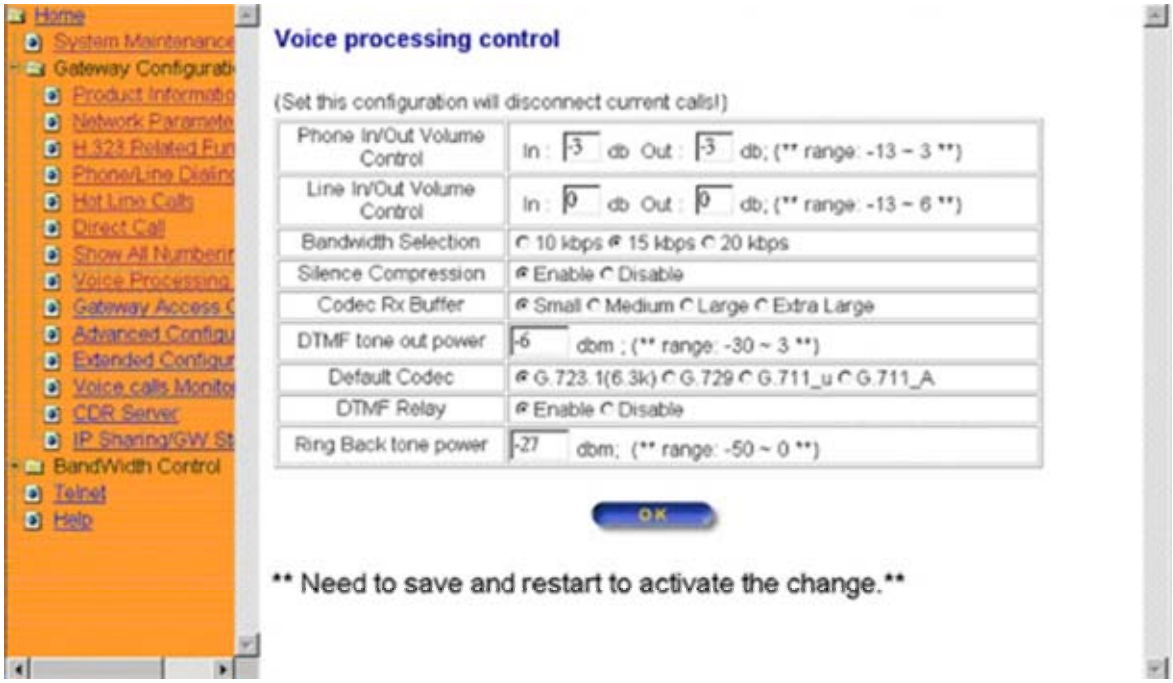


Steps:

- Click “Show All Numbering Plan” in left-side menu.

9.3.9 Voice processing control

This selection is to configure the Gateway and adjust any voice related parameters. Please do not change any default settings if you are not sure about the meanings of functions. The following page is the configuration page when “Voice Processing Control” has been selected:



Steps:

- Click “voice processing Control” in left-side menu.
- Input the correct value, and do the needed selection.
- Press “OK” button.

The following will explain the meanings of all parameters:

Phone In/Out Volume Control:

This function is used for the control of the phone volume. The range is –13dB to 3dB and the default value is –6 dB. When the value is increased, the volume will be increased accordingly. The " **In**" direction is from Gateway to phone set, and the "**Out**" direction is from phone set to Gateway.

Line In/Out Volume Control:

This function is used for the control of the line volume. The range is –13dB to 3dB and the default value is –6 dB. When the value is increased, the volume will be increased accordingly. The " **In**" direction is from Gateway to phone set, and the "**Out**" direction is from phone set to Gateway.

Bandwidth Selection:

This selection is used to choose the bandwidth required in the TCP/IP network. The IP headers are included in the bandwidth. The required bandwidth is dependent on the voice length sent for each packet. The bigger the bandwidth is, the smaller the voice length and hence the smaller the voice delay will be. For 20 kbps, packet is sent every 30 ms and it has 24 bytes of data in payload. For 15 kbps, packet is sent every 60 ms and it has 48 bytes of data in payload. For 10 kbps, packet is sent every 90 ms and it has 72 bytes of data in payload. The maximum bandwidth selection will have the minimum voice delay.

Silence Compression:

If this function is enabled, when silence is occurred for a period of time, no data will be sent across the network during this period in order to save bandwidth.

Codec Rx Buffer:

The Rx buffer is also called the jitter buffer. This buffer is used to decrease the effect of voice packet jitter (delay variation) caused by the network. When the size of this buffer is increased, the jitter effect will be decreased.

DTMF tone out power:

After the VoIP call is connected, when you dial a digit, this digit is sent to the other side by DTMF tone. If the voice path is through many stages (e.g. many PBX), the DTMF tone could be too small to be recognized by the other side. You can adjust this DTMF tone power to increase the recognition. The range of this option is –30 dBm to 3 dBm and the default value is –6 dBm.

Default Codec:

The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are four kinds of Codecs, G.723, G.729, G.711_u and G.711_A. The default value is G.723.

DTMF Relay:

After the VoIP call is connected, when you dial a digit, this digit is sent to the other side by DTMF tone. There are two methods of sending the DTMF tone. The first is "in band", that is, sending the DTMF tone in the voice packet. The other is "out band", that is, sending the DTMF tone as a signal. Sending DTMF tone as a signal could tolerate more packet loss caused by the network. If this selection is enabled, the DTMF tone will be sent as a signal.

Ring Back tone power:

When a call is made from the other side, the other side will send back a tone to inform us, it is called "ring back tone". The power of ring back tone will influence the correctness of judging the busy tone. The range is –50dBm to 0 dBm, and the default value is –27 dBm.

9.3.9.1 Settings for Console/Telnet only

7 Voice processing Control.

7-9 **Disconnect All Current Calls**.

This function can let gateway manager to disconnect all active calls of the line ports. Only the calls in the line ports can be disconnected.

9.3.10 Gateway Access Control

The configuration will let you change the password of web browsing and let the Gateway to deny some calls from specific IP addresses.

Steps:

- Click “Gateway Access Control” in left-side menu.
- Enter the new password in both “New Password” and “Confirm Password” fields
- Press “OK” button.

When the “ENABLE” button of “Enable incoming IP Check” is clicked, you can add items for incoming IP check.

Notice :

When “Enable incoming IP Check” is enabled, only those IP addresses set in this table are allowed to call into this Gateway. If this function is enabled and the table is empty, all calls are not allowed to call in.

Steps:

- If you want to disable this function, press “DISABLE” button again.
- If you want to add an item, enter the IP address you want to check.
- Press “OK” button to add it.

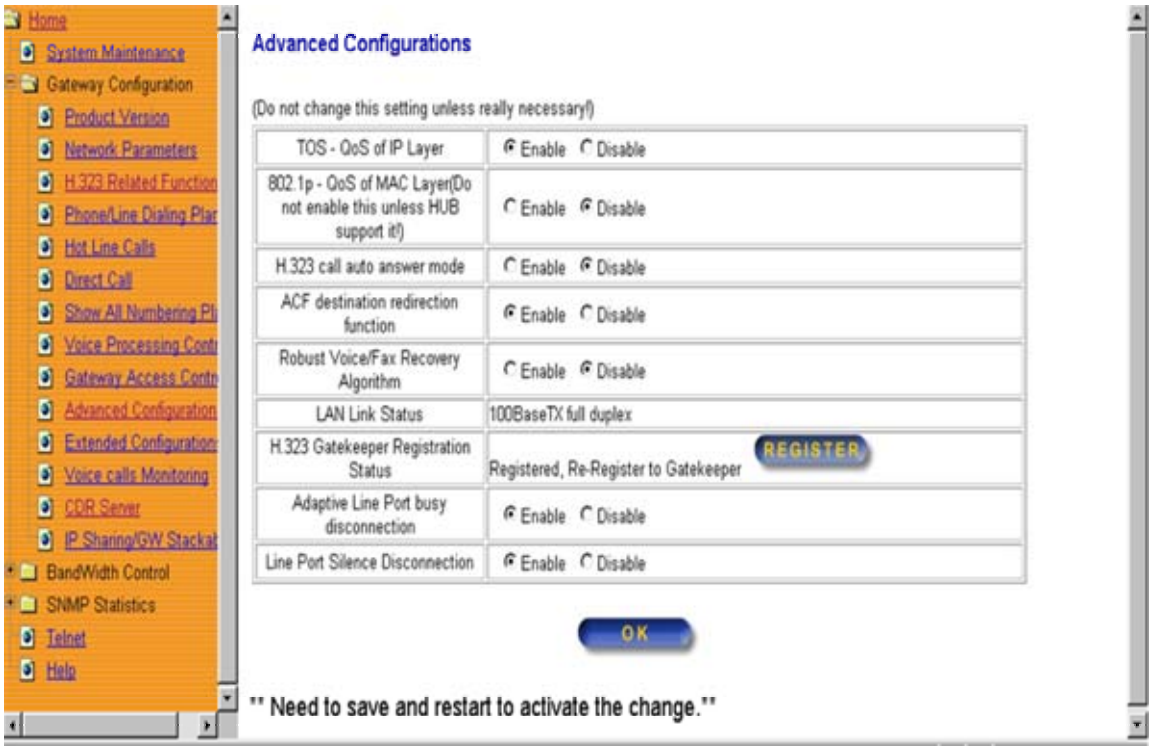
9.3.10.1 Settings for Console/Telnet only

8. Gateway access Control.

8.2. Change the Console/Telnet login Password.
8.4. Choose to Disable Browser Function.
8.5. Choose to Disable Telnet Function.

9.3.11 Advanced Configurations

There are some advanced configurations about the Gateway, and they can be set in this page. The following page will be displayed when the "Advanced Configuration" selection is clicked:



Steps:

- Click "Advanced Configuration" in left-side menu.

TOS - QoS of IP Layer:

This selection is to enable the IP layer “Type of Server” QoS function. This function can ensure voice quality if the network can support IP layer QoS.

802.1p - QoS of MAC Layer:

To enable this function, you must have this Gateway connected to a switching hub supporting 802.1p. Do not enable this function if the hub/switch did not support 802.1p.

H.323 call auto answer mode:

When a VoIP call is incoming, the Gateway will ring a specific phone set. The H.323 call signaling part could be connected or alerting during this ringing period. If this selection is enabled, the H.323 signaling part is connected during the ringing period. The benefit of this situation is that the remote side could hear the status of the specific port. That is, the remote side will hear ring back tone if the Gateway is really ringing the phone set. If the phone set is busy, the remote side will hear busy tone. The disadvantage of this situation is that the H.323 connected time is not the real voice call connected time. So, if billing is recorded for this Gateway, this function should be disabled.

ACF destination redirection function:

If this function is enabled, the Gatekeeper could translated any called number into any other number. This could give the gatekeeper more dialing plan flexibility.

Robust Voice/Fax Recovery Algorithm:

When this function is enabled, the quality of the voice/fax is boosted. But enabling this function will increase the bandwidth usage about 4 kbps per channel.

LAN Link Status:

This selection is for displaying the LAN interface status.

Adaptive Line Port busy disconnection:

When a call has been hanged up from the line port connected to a PBX, the PBX will send a busy tone to the Gateway. The Gateway will automatically disconnect the call when receiving the busy tone. The function must be enabled.

Line Port Silence Disconnection:

If this function is enabled, a connected call will be disconnected if two-way silence is detected for a period of time (30 seconds) for the line port.

9.3.11.1 Settings for Console/Telnet only

9. Advanced Configurations.

9-7 Disable H.245 Fast Capability Exchange.
Please set this to the default value (enabled).

9-b Run Line Port Busy Tone learning.

This function can let the gateway learn some special busy tone that can not be learned by the gateway automatically, for example, busy tone with very long on/off duration(longer than 1 second). Normally, the user does not need to do this learning.

9-c Run Line Port Ringing Tone learning.

This function is provided for called party off-hook detection for the line port. When a VoIP call is incoming from other gateway and called through the line port to a phone set in the PSTN network, this gateway can know when the called phone set is off-hooked by detecting the alerting (ringing) tone. The ringing tone learning can remember two kinds of ringing patterns. It can remember “two cycle” ringing pattern.

This function can be used to generate correct billing record if the line port is connected to PSTN line. In order to let this function work correctly, the H.323 auto-answer mode must be disabled and the “Ringing tone detect duration” must be suitably set (about 15 seconds).

9-d Enable the Line Port Power dynamic reduction ability.

This function is designed to help reducing some failed busy-tone detection problem caused by the echoed energy, but enable this function will cause some uncomfortable voice quality. For almost applications, disable this function.

9-e Set Ringing Tone detect duration.

This function is provided for called party off-hook detection for the line port. When a VoIP call is incoming from other gateway and called through the line port to a phone set in the PSTN network, this gateway can know when the called phone set is off-hooked by detecting the alerting (ringing) tone. This ring tone must first be learned by 9-c.”run line port ringing tone learning”. This detect duration must be longer than the duration the PSTN network generate the ringing back tone.

9.3.11.2 Line Port (FXO) Characteristics

The line ports in all the gateway series have the following characteristics:

1. Busy tone adaptive learning/disconnection (tone duration < 900 ms).
2. Busy tone manual learning/disconnection (tone duration < 3000 ms).
3. Alerting tone manual learning can learn one cyclic or two cyclic patterns.
4. Off hook detection:
    a. If user off hook immediately, will be detected after a “ring tone detection duration”.
    b. If user off hook after some alerting tone, will be detected after a “ring cyclic” (max of [ring-on, ring-off]).
5. Alerting forever detection: After alerting duration is longer than 90 seconds, the FXO port will automatically disconnect it:
    a. Even if altering tone not learned.
    b. Even if the alerting pattern is one cyclic or two cyclic
6. If called side disconnected before 13 seconds, the FXO busy tone disconnection would work after 13 seconds (to prevent dial tone like busy tone problem).

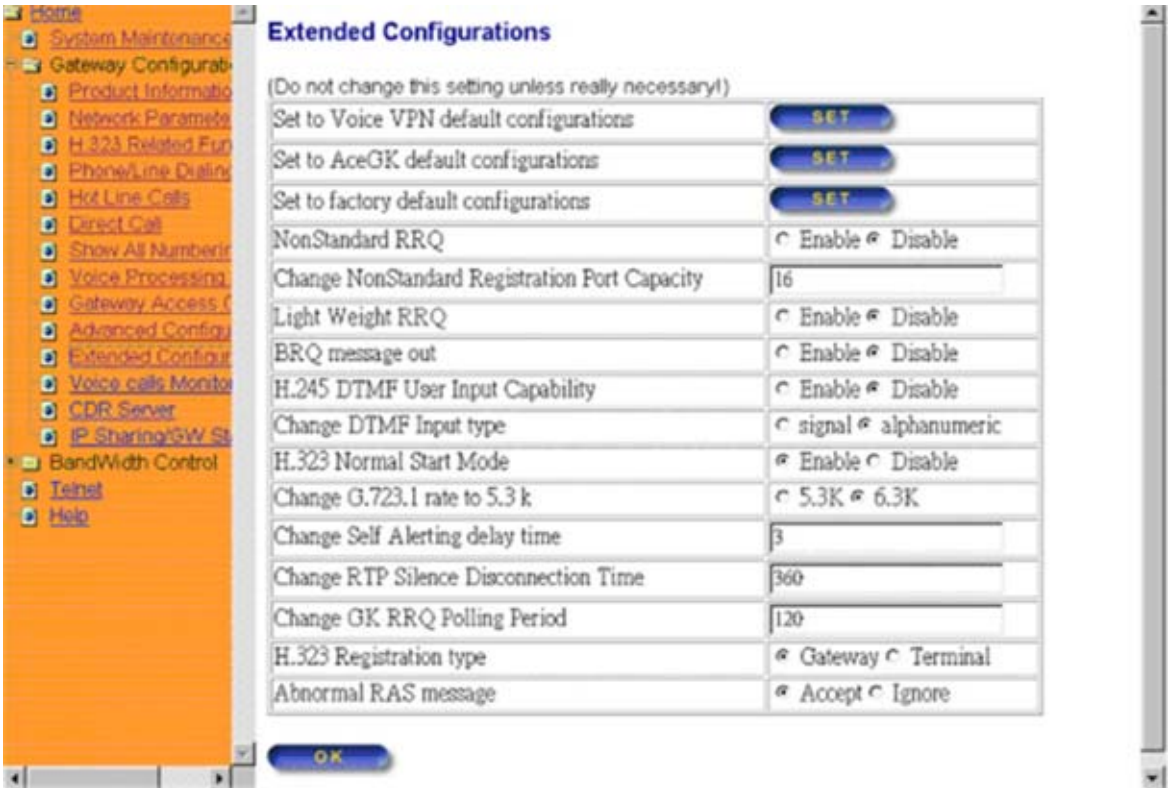
9.3.11.3 Phone Port (FXS) Characteristics

The phone ports in all the gateway series have the following characteristics:

1. FXS alerting tone (1000, 2000) will not last longer than 90 seconds. (Disconnected after 90 seconds)
2. When the phone set (connected to FXS port) is off hooked, it will go to busy tone (250, 250) after 10 seconds, will power deny 400 ms after 30 seconds (this will notify a PABX to disconnect) and busy tone forever.
3. When FXS is disconnected, it will generate busy tone (250, 250) immediately.
4. When FXS is connected, it will do a current reversal (1). (Reversed polarity)
5. When FXS is disconnected, it will do a current reversal (0) again. (To normal polarity)

9.3.12 Extended Configurations

The Gateway has some Extended configurations that can be set in this page. The following page will be shown when the "Extended Configuration" selection is clicked:



Steps:

- Click "Extended Configurations" in left-side menu.

NonStandard RRQ:

This selection is to enable the RRQ message containing nonstandard elements (Non Standard Identifier) for special interoperability purpose. Should be disabled for most cases.

Change NonStandard Registration Port Capacity:

This selection is to set the special "port capacity" for this gateway for special interoperability purpose. This setting is no effect if "NonStandard RRQ" is disabled.

Light Weight RRQ:

This selection can let the registration message (RRQ) contains only necessary information for keep alive purpose; this could save a few network bandwidth. Default is disabled.

BRQ Message Out:

This selection can let the Gateway send out a BRQ (Bandwidth Request) message to the gatekeeper when the Gateway is really connected on the voice channel. The gatekeeper could use BRQ message for billing purpose.

H.245 DTMF User Input Capability:

This selection can let the Gateway contain "DTMF capability" in the H.245 capability exchange message. This capability element is for special interoperability purpose with other gateway. Default is disabled.

Change DTMF Input Type:

The DTMF tone could be sent during a voice call by using the H.245 user-user message. This selection could further select the carrying method of using "signal" format or "Alphanumeric" format in this DTMF message. The default value is "Alphanumeric" format.

H.323 Normal Start Mode:

This selection could force the Gateway to use normal start mode or fast start mode when establishing a VoIP call. Many other gateways only support normal start mode, enable this selection when it is necessary. The default is disabled (using fast start mode).

Change G.723.1 rate to 5.3k:

This selection can force the G.723.1 codec to use 5.3k bps speeds instead of default 6.3k speeds.

Change Self Alerting delay time:

This setting is to set the ring-back tone delay time when a voice call is proceeding. Too short delay could confuse the caller. The default is 3 seconds.

Change RTP Silence Disconnection Time:

This selection could let the Gateway polling the voice packets (RTP packets) to make sure that the connected two parties are still under normal operation. If one side is powered down during the conversation, the Gateway will do a forced disconnection at the other side after this set time duration.

Change GK RRQ Polling Period:

The value is based on seconds (e.g. 120 means 120 seconds). The gateway will register to gatekeeper after a polling period of time. When the setting value is 120 then the gateway will register to gatekeeper every 120 seconds.

H.323 Registration type:

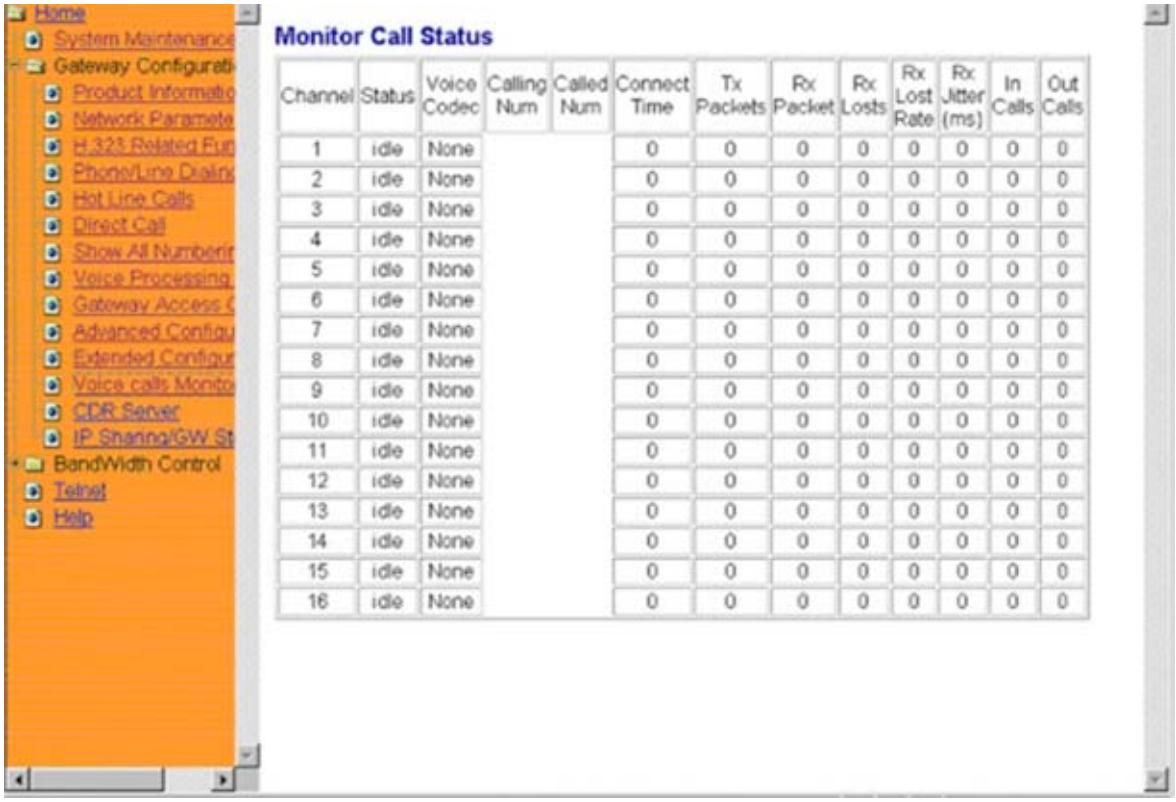
There are 2 choices for this setting. “Gateway” means it will act as the VoIP gateway. “Terminal” means it will act as the IP phone terminal.

Abnormal RAS message:

When some RAS messages from gatekeeper is unrecognizable, the gateway can choose “Accept” or “Ignore” for responding to the abnormal RAS message.

9.3.13 Voice calls Monitoring

This selection will display concurrent call status of this Gateway. This status is refreshed every 5 seconds.



Channel	Status	Voice Codec	Calling Num	Called Num	Connect Time	Tx Packets	Rx Packet	Rx Losts	Rx Lost Rate	Rx Jitter (ms)	In Calls	Out Calls
1	idle	None			0	0	0	0	0	0	0	0
2	idle	None			0	0	0	0	0	0	0	0
3	idle	None			0	0	0	0	0	0	0	0
4	idle	None			0	0	0	0	0	0	0	0
5	idle	None			0	0	0	0	0	0	0	0
6	idle	None			0	0	0	0	0	0	0	0
7	idle	None			0	0	0	0	0	0	0	0
8	idle	None			0	0	0	0	0	0	0	0
9	idle	None			0	0	0	0	0	0	0	0
10	idle	None			0	0	0	0	0	0	0	0
11	idle	None			0	0	0	0	0	0	0	0
12	idle	None			0	0	0	0	0	0	0	0
13	idle	None			0	0	0	0	0	0	0	0
14	idle	None			0	0	0	0	0	0	0	0
15	idle	None			0	0	0	0	0	0	0	0
16	idle	None			0	0	0	0	0	0	0	0

Steps:

- Click “Voice Call Monitoring” in left-side menu.

9.3.14 CDR Server

The Gateway can generate call detail records of the VoIP calls and send them to a CDR server. The only thing what you should do is to set a IP address of CDR server. In case the CDR server is not running, the operation of the Gateway is not affected. The call detail record includes calling/called gateways IP, calling/called telephone numbers and call duration, … etc. The CDR server is a Windows application freely provided by antek.

CDR Control:

This gateway can be fully controlled by the CDR server if the "CDR Control" is enabled. If it is enabled, the gateway must connect to the CDR server and the CDR server must enable this gateway, otherwise this gateway cannot make any calls. If the "CDR Control" is enabled, but no CDR server is connected, this gateway cannot make any calls.

9.3.15 IP Sharing/GW Stack-ability (VSP-Series only)

For the requirement to operate in many different kinds of network environment, it is very possible that only one IP address is available for VoIP GWs (Gateway). For example, you could combine 2 or more VoIP GWs together, while there is only one IP address for you. We named this special function as "GW Stack-ability". Another example is that you want to integrate the NAT (Network Address Translation) of your private network and VoIP GW together. Our device can share the same IP address of NAT without any intrusiveness by using only 50 ports of it. It is call the "IP Sharing" function. We will have detail description about it below.

This selection can disable or enable the IP Sharing/GW Stack-ability function of the Gateway. If the function is enabled, the submenu item (Set the Base-Port) will work to constrain the utilized ports that can only be accessed by this device within the range from Base-Port to "Base-Port+49". Notice that other devices must avoid this range of ports. If this function is disabled, it acts as a regular Gateway without any difference.

✧ Notice:

1. Enabling this function, users must directly connect from the LAN port to the device with the same IP address what you want to share.

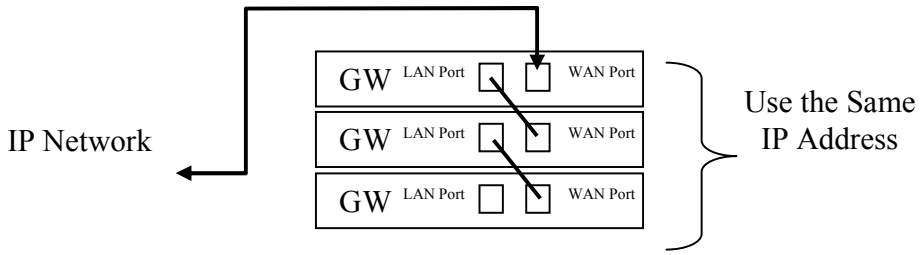
2. Once this function is enabled, the IP address of gatekeeper must be specified. This function can only operate correctly with the cooperation of gatekeeper.

3. Users could assign the same dialing number to different VoIP devices with IP sharing function, if it cooperate with antek-gatekeeper, which is specially implemented an auto-hunting function. The Gatekeeper could hunt different GWs; even the same number is dialed.

4. If this function is activated, users can only http-browse or telnet the devices from the WAN side instead of the LAN side.

9.3.15.1 Stackable GWs

Following figure is the demonstration of stack-ability. And there are several important steps for configuration described below.



Step 1: Set all of the stacked devices by the same IP address say “168.92.1.1”.

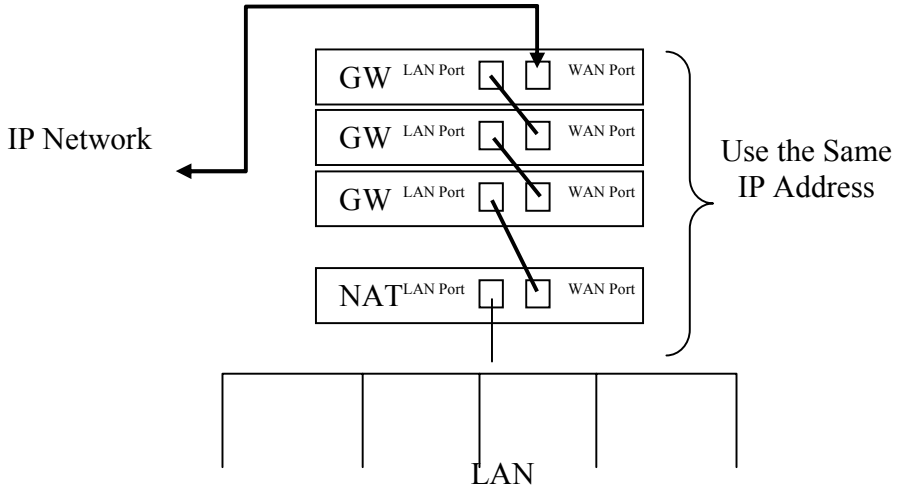
Step 2: Enable the IP Sharing/GW Stack-ability.

Step 3: Set the Base-Port. For example, users may set the Base-Port of first device equal to 50000. It will consume ports form 50000 to 50049. And set 50050 for the next one, it will consume ports from 50050 to 50099. Then set the last one by 50100. Notice that you have to avoid the condition of ports collision from these devices with the same IP. Be sure that each device consumes different range of ports.

Step 4: Save the configurations and restart systems.

9.3.15.2 IP Sharing (1 IP Address Only)

Following figure is the demonstration of IP sharing. There is only 1 IP address available. The important steps for configuration described below.



Step 1: Set all of the VoIP devices by the same IP-address of NAT.

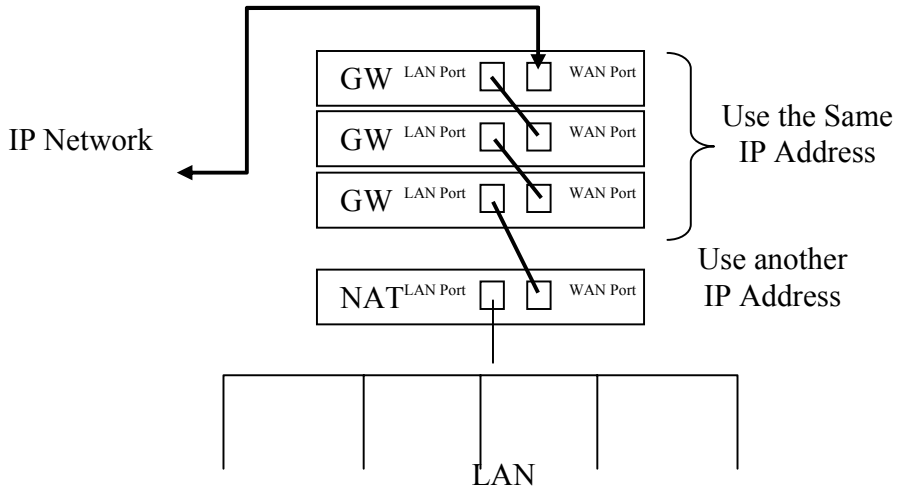
Step 2: Enable the IP Sharing/GW Stack-ability.

Step 3: Find out a free port range from NAT that NAT will never use these ports, say 50000 ~ 50200. Then set the Base-Ports within this range. For example, set the Base-Port equal to 50000 for the first device, 50050 for the second one, and 50100 for the other one.

Step 4: Save the configurations and restart systems.

9.3.15.3 IP Sharing (more than 1 IP Address available)

Following figure is the demonstration of IP sharing with more than 1 IP address available. For convenience, you have better reserve 1 IP for VoIP devices only. And the computer network uses other IP addresses. The important steps for configuration described below.



Step 1: Set all of the VoIP devices by the same IP-address, say “168.92.1.1”.

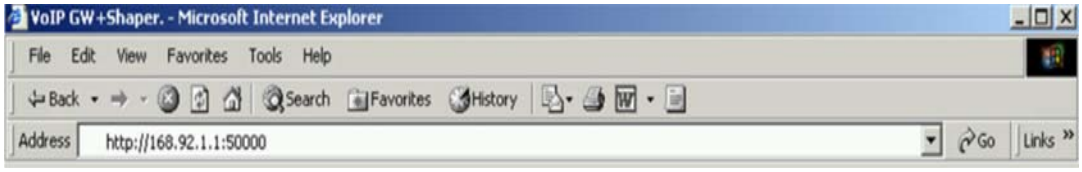
Step 2: Enable the IP Sharing/GW Stack-ability.

Step 3: Set the Base-Port. For example, set the Base-Port equal to 50000, 50050 and 50100 for each one of these VoIP devices.

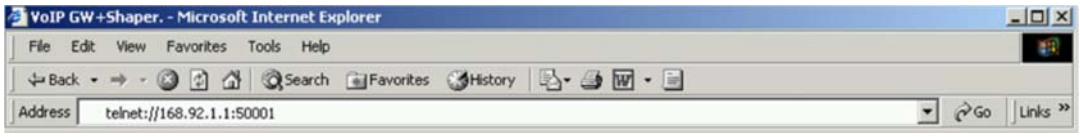
Step 4: Save the configurations and restart systems.

9.3.15.4 IP-Sharing Management and Maintenance

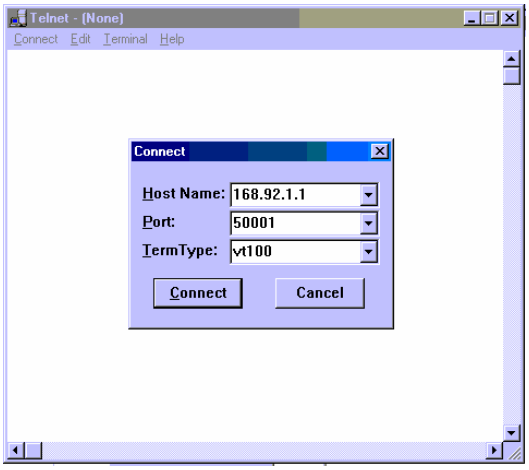
When the Base-Port setting has been done, system will display the ports number of Http, Telnet, and RAS automatically. Because these ports are different from the default ports usually used, users have to clearly specify the ports for accessing these services. You may use the command of IE browser, such as "http://168.92.1.1:50000", to browse your Gateway in the condition that its IP-address is 168.92.1.1 and Base-Port equal to 50000.


VoIP GW+Shaper. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://168.92.1.1:50000
Go Links

For telnet communication, there are two ways that user can connect it. The first one is using the command of IE browser, such as "telnet://168.92.1.1:50001", to connect it through telnet protocol.


VoIP GW+Shaper. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address telnet://168.92.1.1:50001
Go Links

The second approach is using the telnet software tools with clearly specified the port number equaling to "Base-Port + 1", for example 50001.



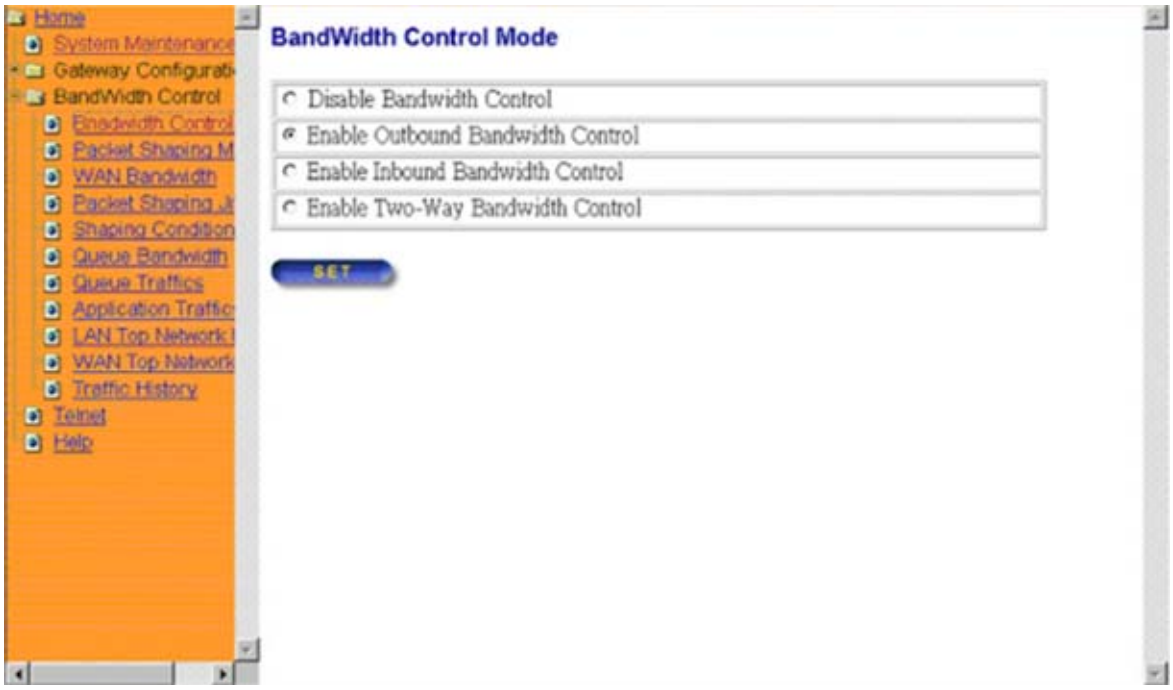
9.4 Bandwidth Control (VSP-Series only)

The Gateway has Bandwidth control function. It can control both of the Inbound/Outbound Bandwidth for the network traffics.

9.4.1 Enable/Disable Bandwidth Control.

This selection can disable or enable the bandwidth control function of the Gateway for both of the Inbound/Outbound network traffics. If the function is enabled, the submenu item (Set Priority Queue Bandwidth) will work to constrain the bandwidth of each priority queue. If this function is disabled, all packets are passing through this Gateway at full speed. The default is "Disable".

For good voice quality, gateway must enable the two-way bandwidth control function and specify correct WAN bandwidth.

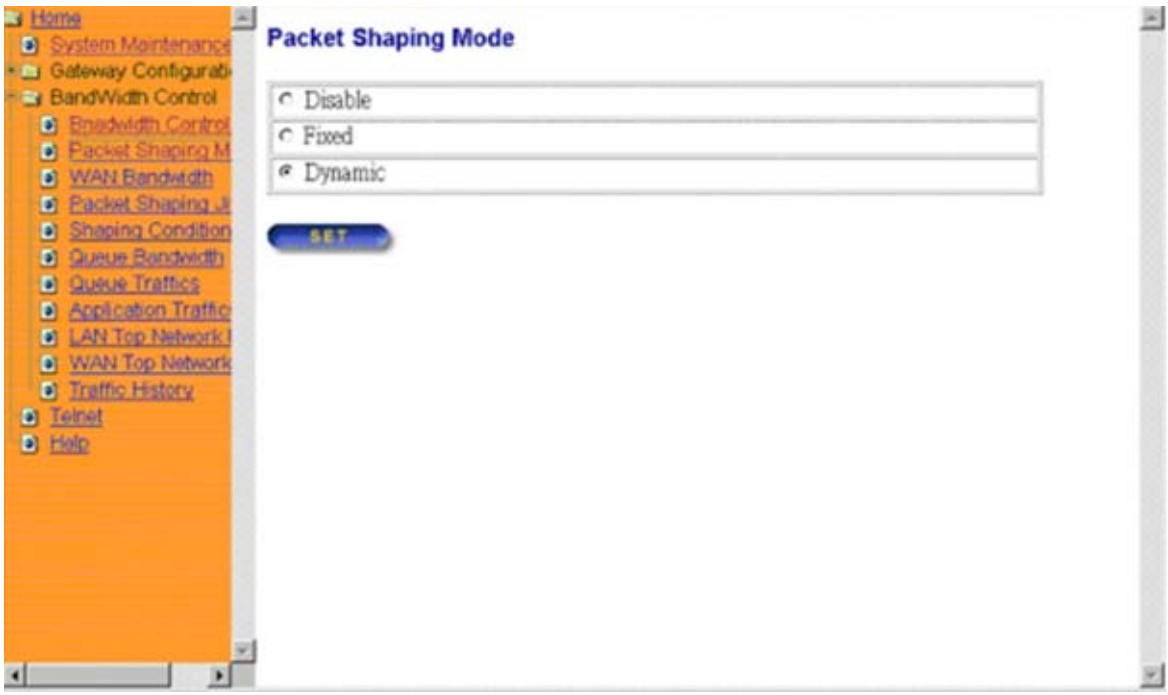


Steps:

- Click "Bandwidth Control Mode" in left-side menu.
- Choose "Enable" or "Disable" bandwidth control, then press "SET" button.

9.4.2 Set Packet Shaping Mode.

The Gateway can be selected to disable/enable the packet shaping function. If the packet shaping function is disabled, the Gateway will not be able to control the voice latency caused by data traffic. If the packet-shaping mode is set to fixed, the packet traffic is shaped to a limited latency but can cause variable voice latency. Only when the shaping mode is set to dynamic will the Gateway do the best to reduce the voice latency to really improve the voice quality. The default setting is “Dynamic”.

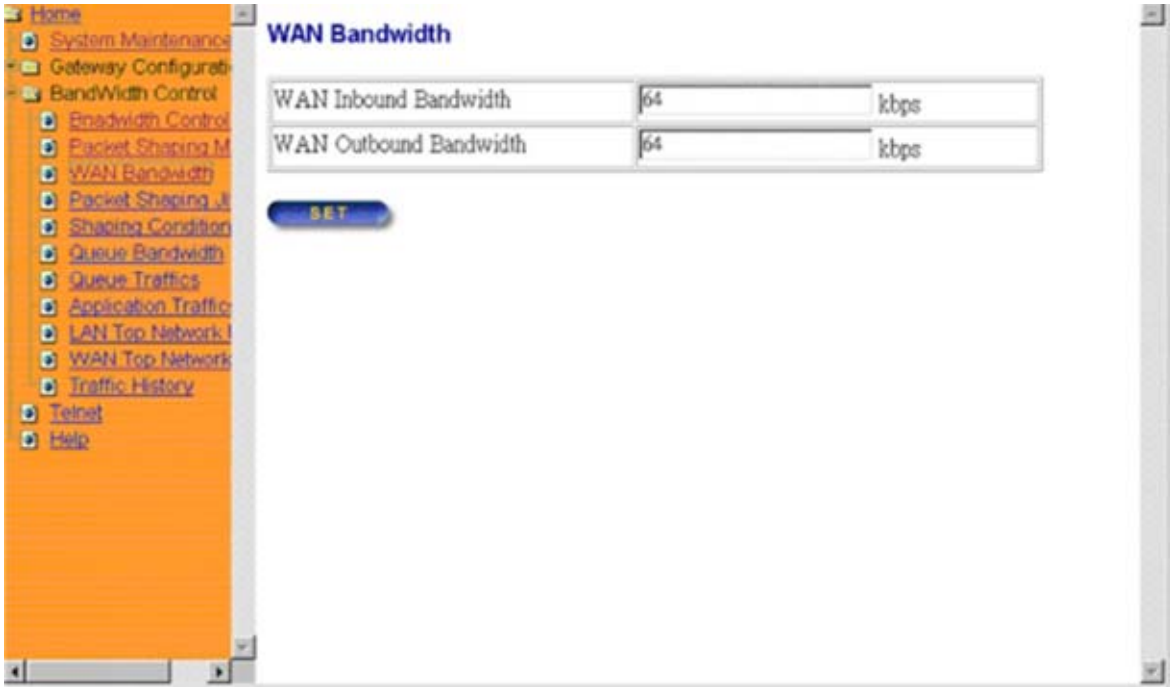


Steps:

- Click “Packet Shaping Mode” in left-side menu.
- Choose “Disable”, “Fixed” or “Dynamic”, and then press “SET” button.

9.4.3 Set WAN Inbound/Outbound Bandwidth.

This setting is to set the real WAN bandwidth. Please correctly set the inbound and outbound bandwidth of the WAN link. If this value is not correctly set, the Gateway will not work well to improve the VoIP voice quality and control the data bandwidth efficiently. The maximum inbound and outbound bandwidth is limited to 2048 kbps.

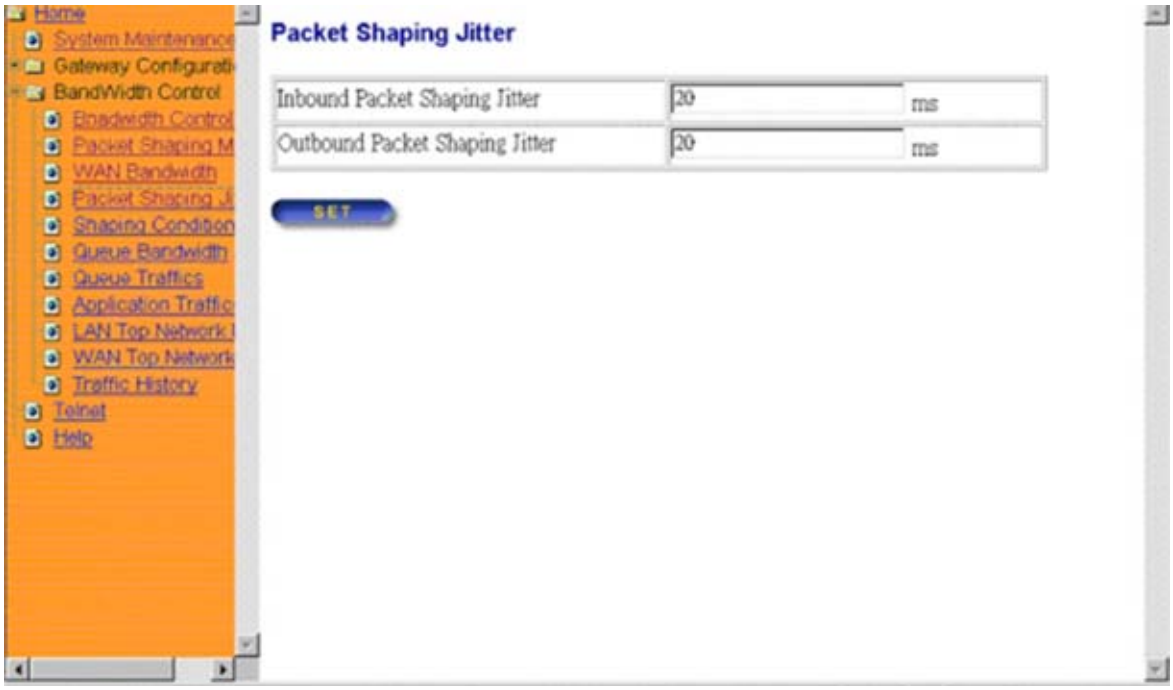


Steps:

- Click “WAN Bandwidth” in left-side menu.
- Key in the inbound and/or outbound bandwidth, then press “SET” button.

9.4.4 Set Inbound/Outbound Packet Shaping Jitter.

This setting is adjusting the packet jitter caused by data traffic. Reducing this value can improve the voice quality (reduce voice latency) and speedup the general application's response time, but a too little value can also reduce the network efficiency. The default value is 20ms. Please do not change the default value unless you can get a better balance between voice quality and network efficiency.



Steps:

- Click "Packet Shaping Jitter" in left-side menu.
- Key in the inbound and/or outbound shaping jitter, then press "SET" button

9.4.5 Set Shaping Conditions.

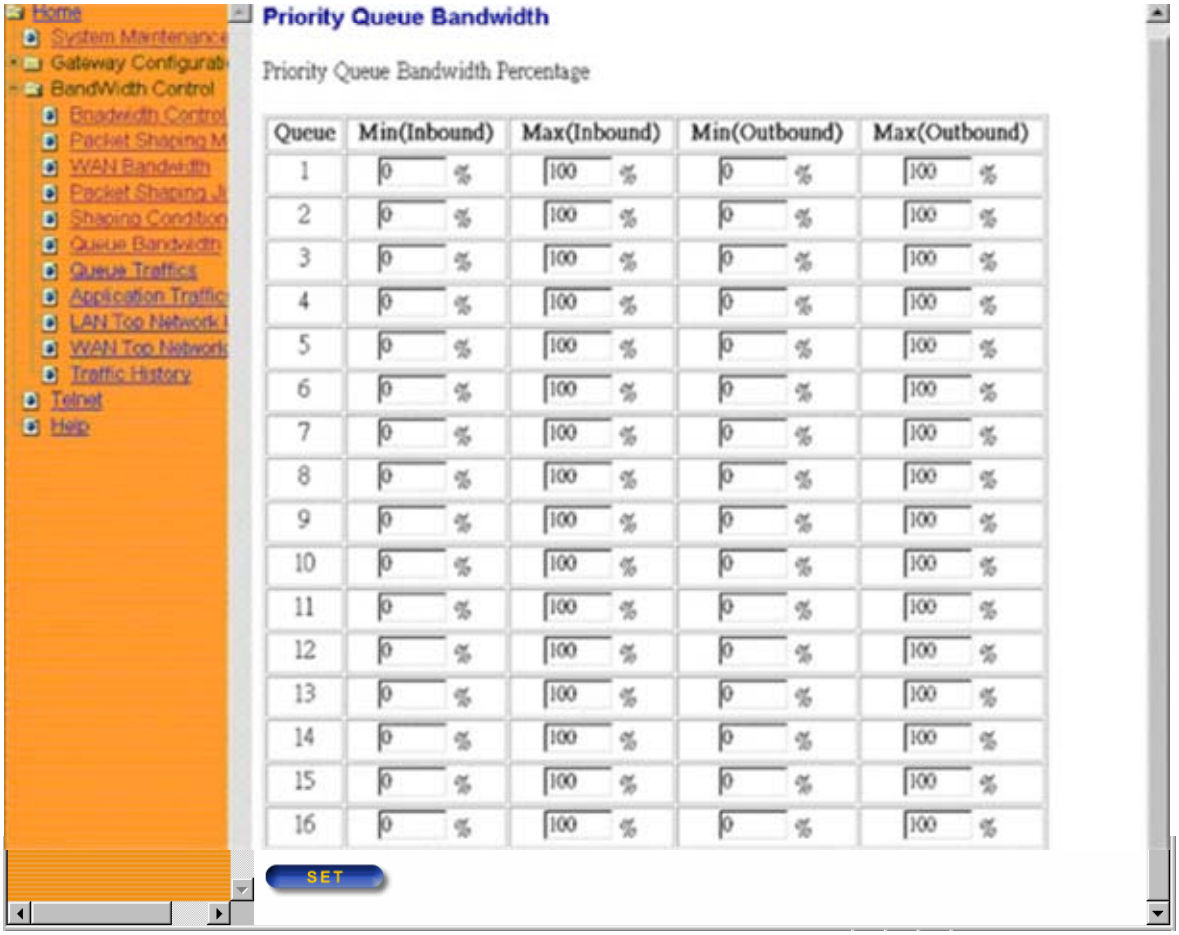
The Gateway can control the packet traffic's bandwidth according to the user defined shaping conditions. The shaping conditions are classifying the packet traffics to some groups by specifying each group's IP address's range, UDP/TCP type, and port range and/or inside/outside conditions. Each group is assigned a priority; different groups can have the same priority. There are totally 16 priorities with priority 1 be the highest priority. Some group's all packets can be discarded by assigned to priority 0. The default priority of any ungrouped packets is 10. Some packets may satisfy multiple group's conditions, in this case, they are mapped to the highest priority group belonged. The bandwidth control of the packet traffics is based on the priority of these shaping conditions. All groups with the same priority are controlled by the following specified priority queue bandwidth. The maximum shaping conditions are 32.

Steps:

- Click "Shaping Conditions" in left-side menu.
- Key in the needed shaping condition, then press "ADD" button.
- If you want to delete condition items, input the start and end item number to delete and then press "DEL" button.

9.4.6 Set Priority Queue Bandwidth.

All groups (by shaping conditions) with the same priority can be assigned same bandwidth range. The bandwidth range is based on the percentage of the inbound and outbound WAN bandwidth. The minimum value of the bandwidth range is the guaranteed minimum bandwidth percentage of the total available WAN bandwidth that can be used by the same priority groups. The maximum value of the bandwidth range is the limited maximum bandwidth percentage of the total available WAN bandwidth that can be used by the same priority groups. The WAN bandwidth is first used by the guaranteed minimum bandwidth percentage of the priority groups. The remaining bandwidth is then dispatched to each priority groups according to the priority (highest priority first) and maximum bandwidth percentage.



Steps:

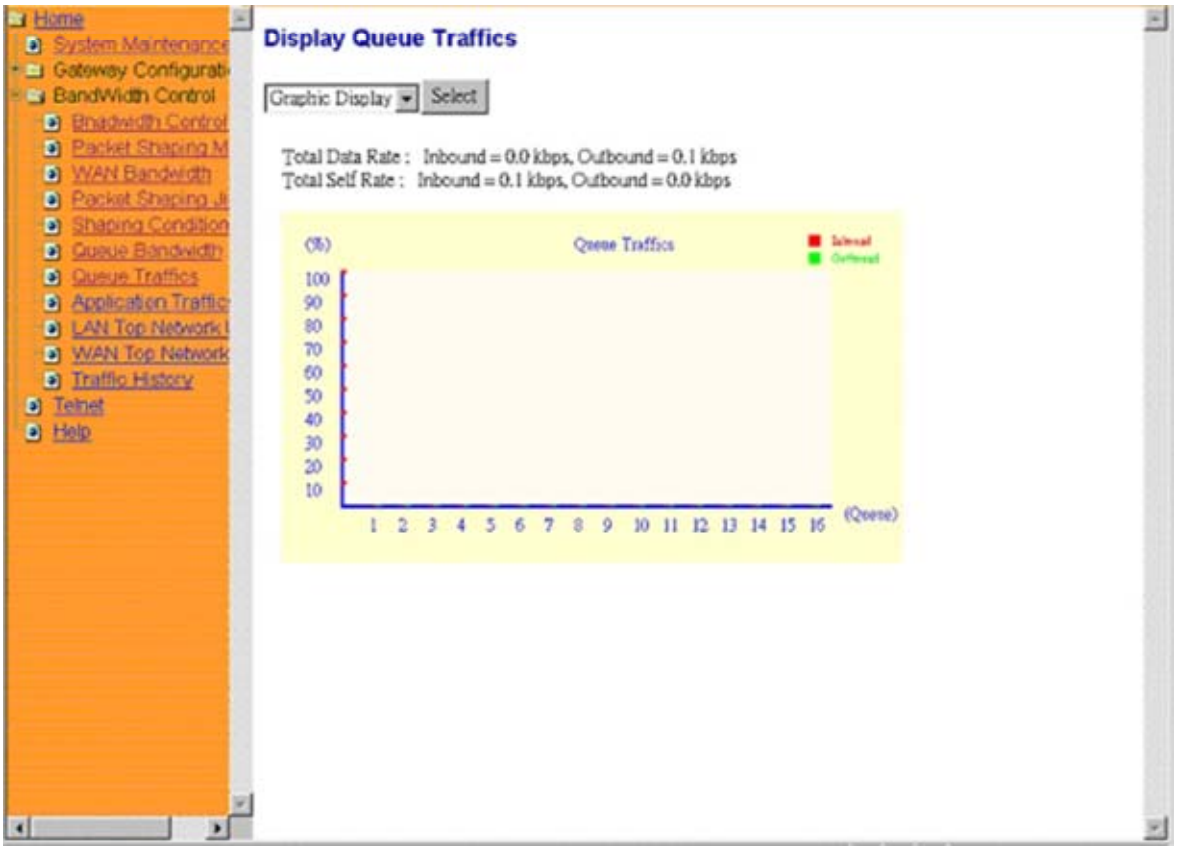
- Click “Queue Bandwidth” in left-side menu.
- Key in the minimum and/or maximum percentage of queue, then press “SET” button.

Notice:

1. The Queue with smaller number has the higher priority than Queue with larger numbers**.**
2. **Bandwidth Fairness:** The bandwidth assigned to each queue is fairly distributed among all the active peers. For example, if 10 PCs belong to a same queue is connecting to the internet through the gateway, but at the some moment, only three of them are sending traffics, the gateway will give 1/3 of the bandwidth to each of the active PCs. This fairness of bandwidth usage is based on the PC, not on each TCP/UDP connection.

9.4.7 Display Queue Traffics

This selection can display the bar graphics/texts of the traffics of each priority groups.

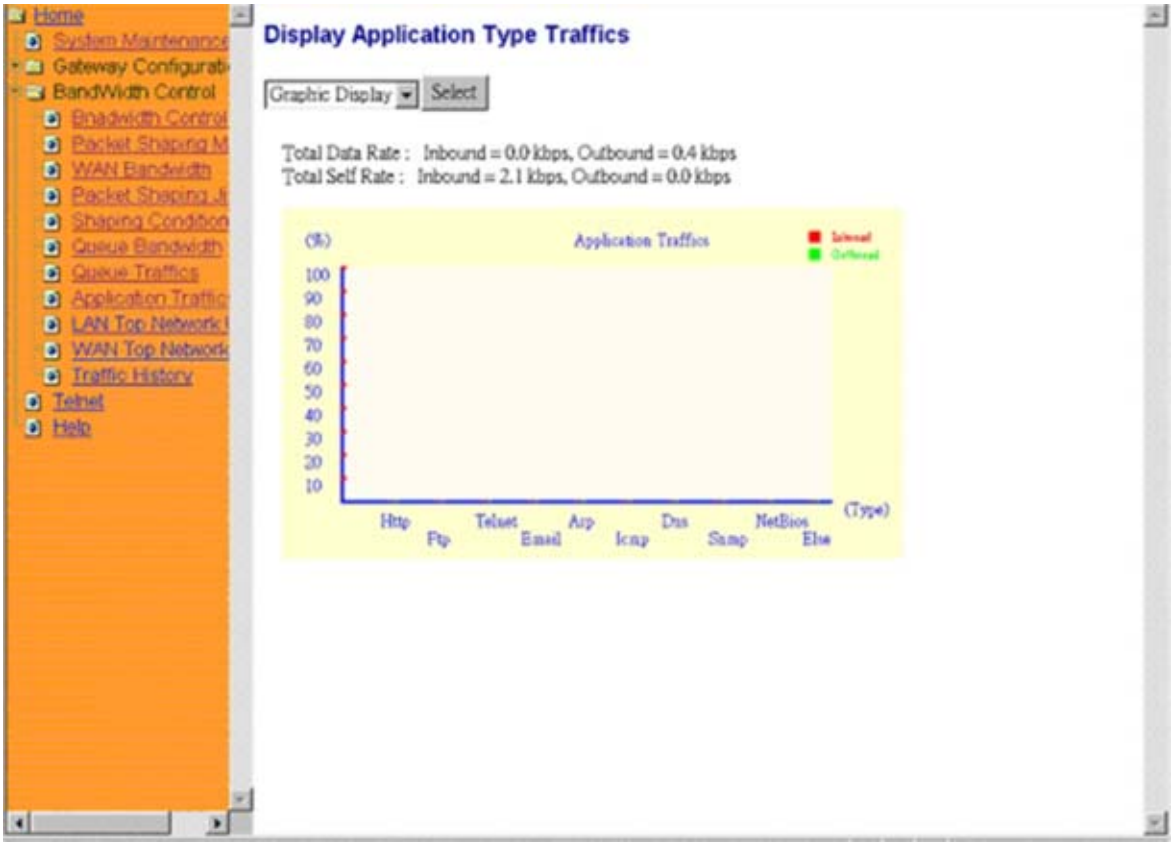


Steps:

- Click “Queue Traffics” in left-side menu.

9.4.8 Display Application Traffics

This selection can display the bar graphics/texts of the traffics of each applications (Web, Ftp, Telnet, ICMP, DNS, Net bios, SNMP, ...).



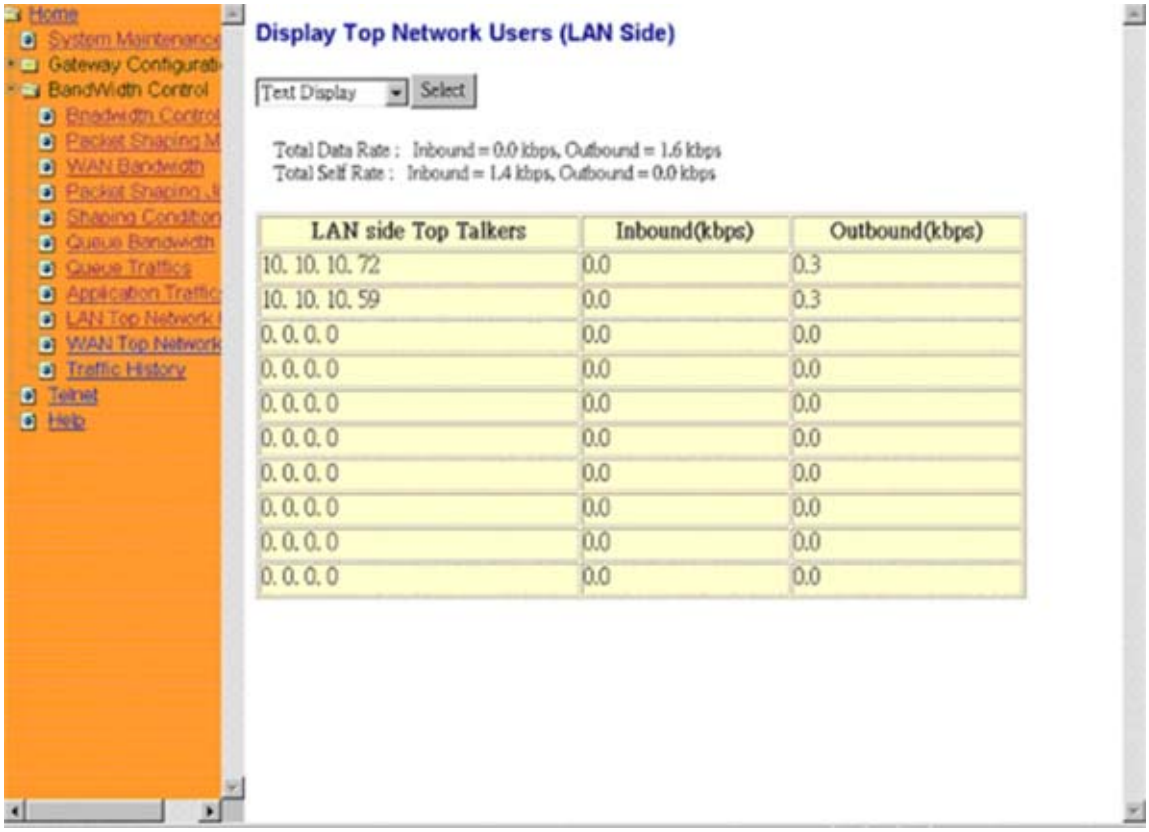
Steps:

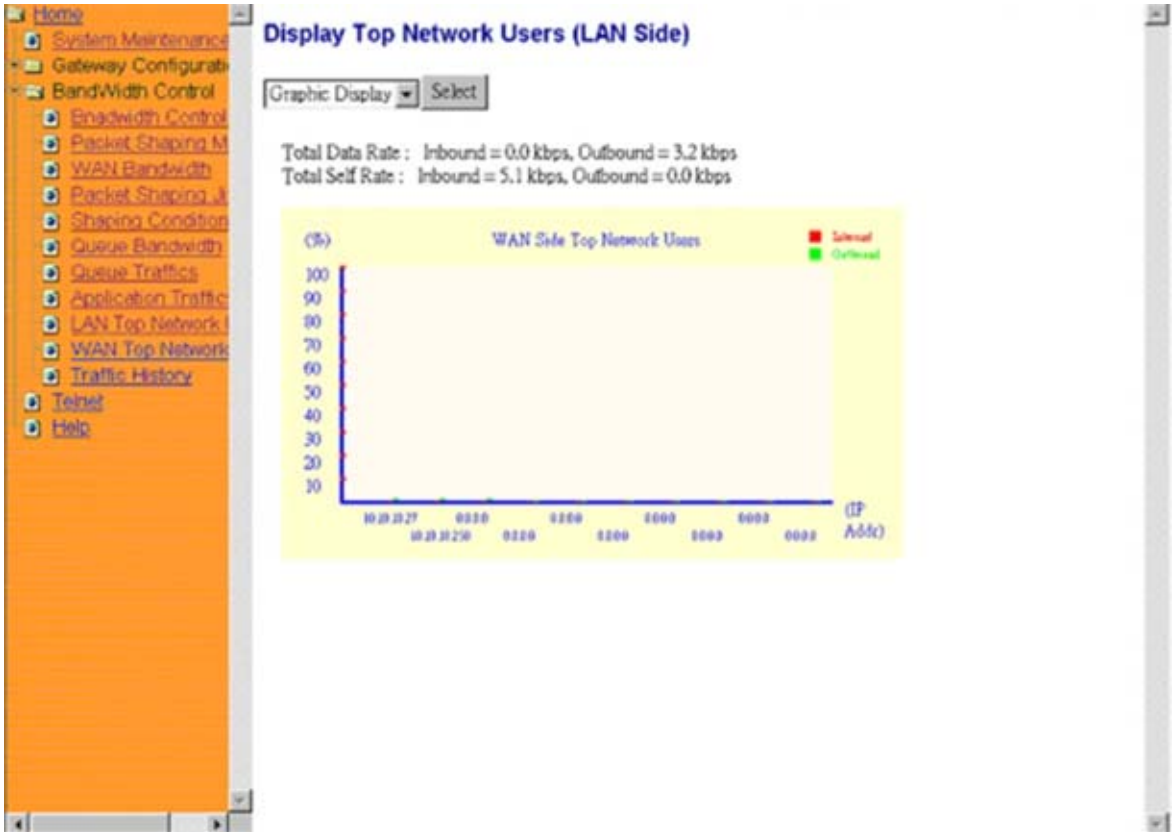
- Click “Application Traffics” in left-side menu.

9.4.9 Display Top Network Users.

This selection can display the bar graphics of the traffics of 10 top network users. The users are considering only inside network users.

9.4.9.1 LAN Top Network User

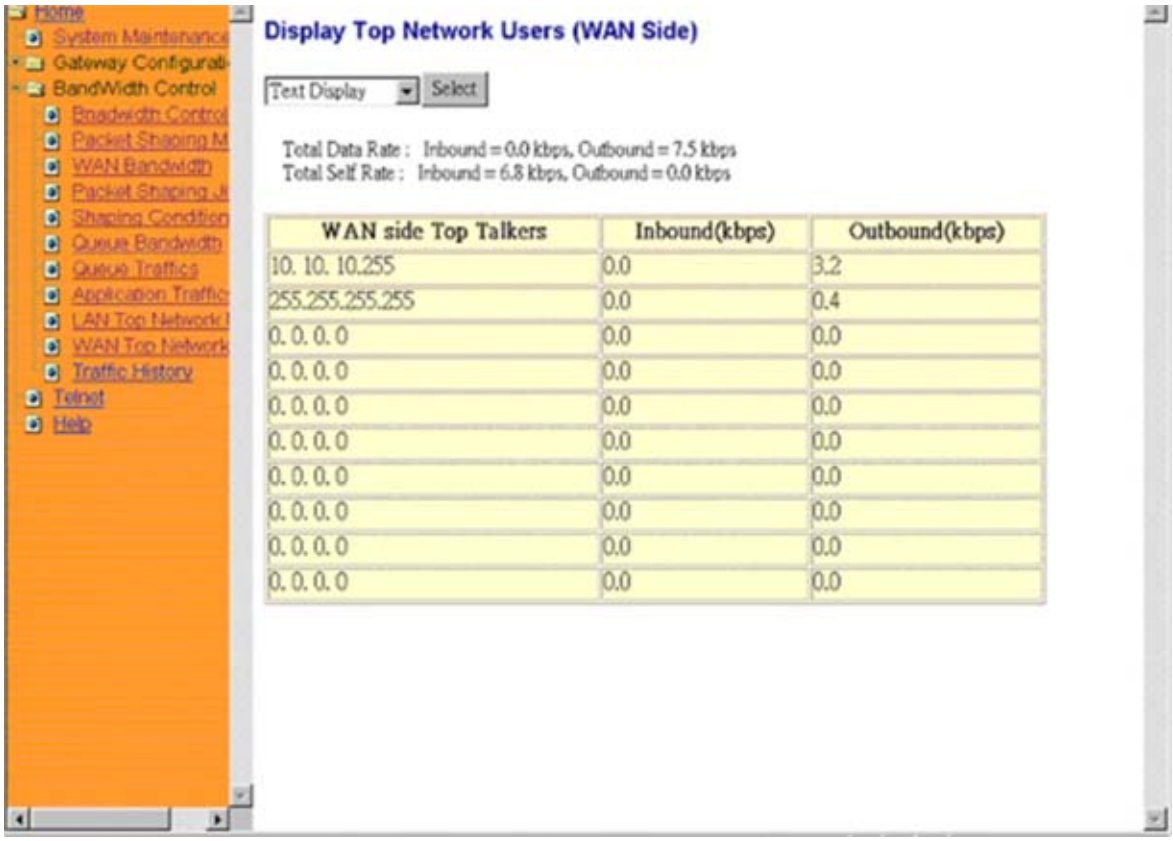


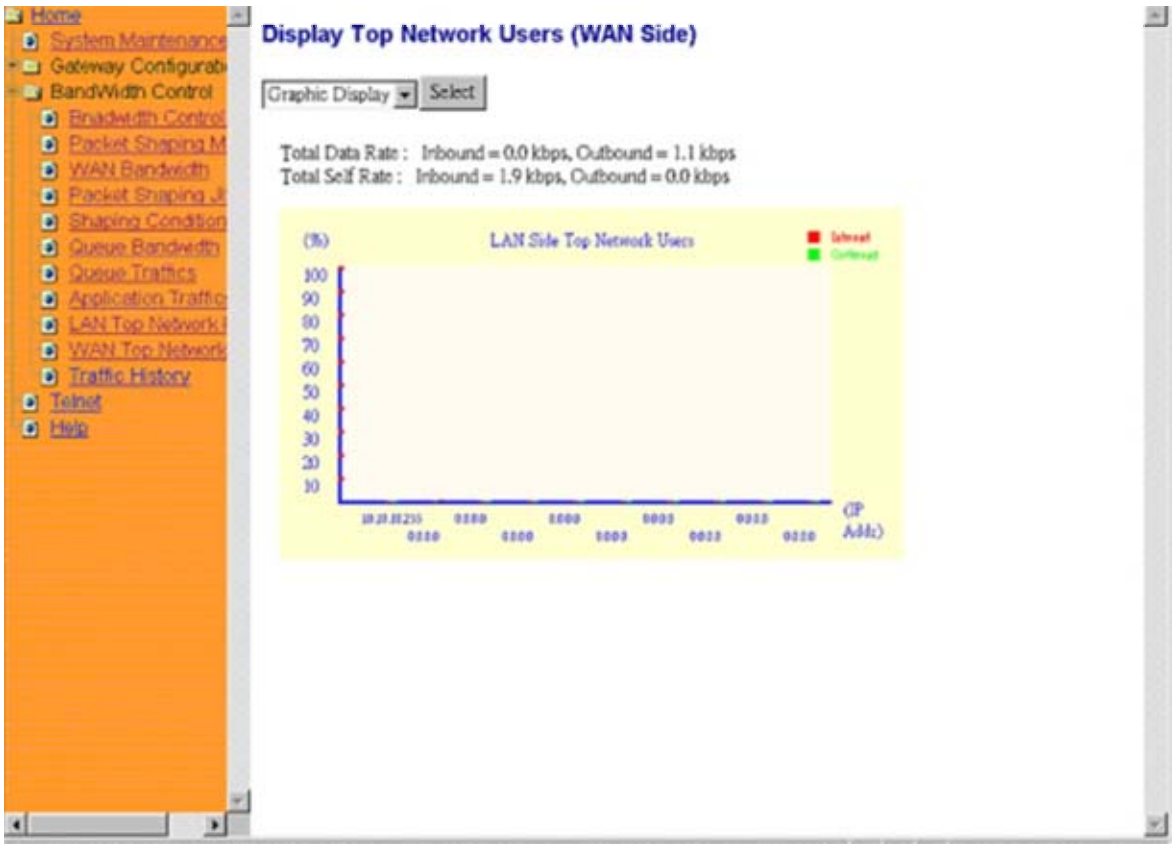


Steps:

- Click “LAN Top Network Users” in left-side menu.

9.4.9.2 WAN Top Network User



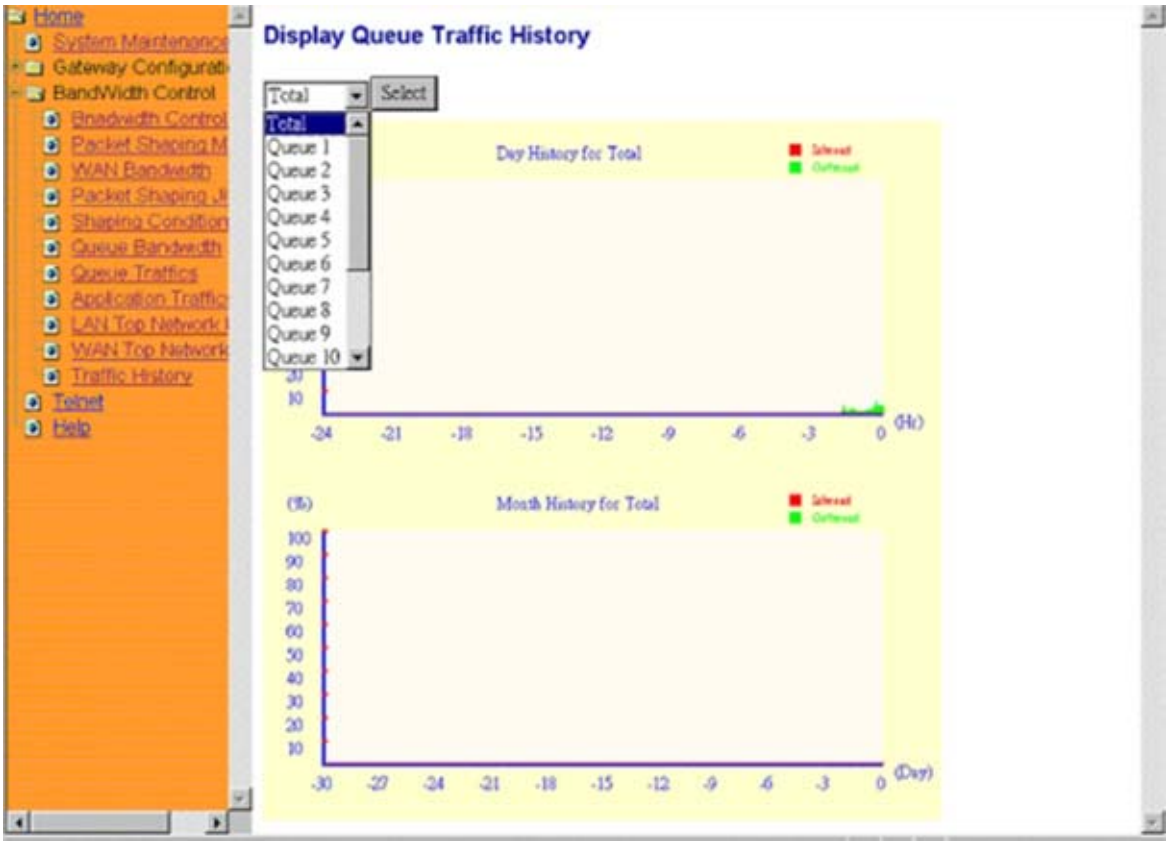


Steps:

- Click “WAN Top Network Users” in left-side menu.

9.4.10 Traffic History

This selection can display the graphics of traffic history of each priority groups. The history includes day history and month history. The day history is displaying the inbound/outbound traffics of each priority groups every 6 minutes before current time. The month history is displaying the inbound/outbound traffics of each priority groups every 3 hours before current time.



Steps:

- Click “Traffics History” in left-side menu.
- You can select a Queue to see its traffic from the pull-down menu.

9.4.11 Configuration Examples:

Example 1:

Shaping conditions: (click on "Shaping Conditions" from left-side menu)

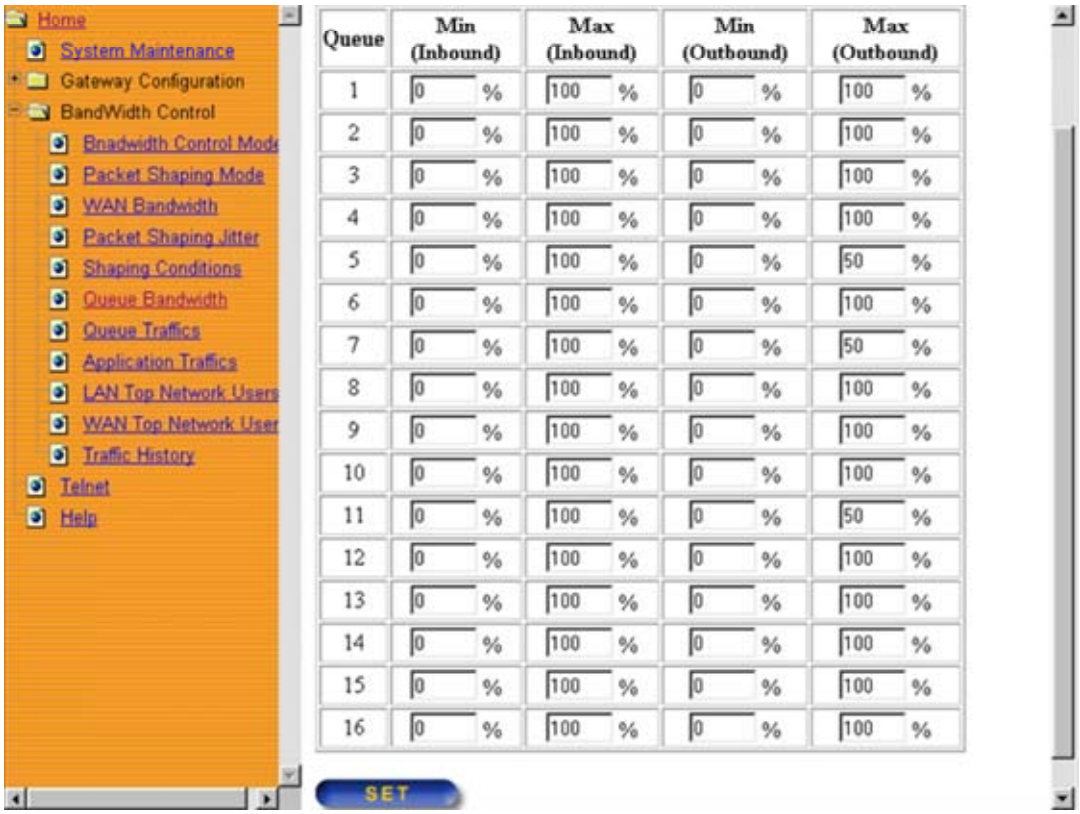
In the above conditions

1. Any packets from/to inner IP 10.10.10.23 will have the priority 5.
2. Any Web packets (with server inside or outside) will have the priority 7. But the web packets from/to 10.10.10.23 still have the priority 5,
3. Any Ftp packets (with server inside or outside) from/to 10.10.10.10 ~ 10.10.10.200 will have the priority 9. But the ftp packets from/to 10.10.10.23 still have the priority 5,
4. The fourth condition will be meaningless, since this condition is a subset of condition 1 and condition 1 has higher priority. All packets satisfying condition 4 are satisfying condition 1 and will have the priority 5.
5. Any other packets not satisfying these conditions will have the priority 10.

Example 2:

Priority Queue Bandwidth: (click on “Queue Bandwidth” from left-side menu)

Suppose the bandwidth assignments of the priority queues are:



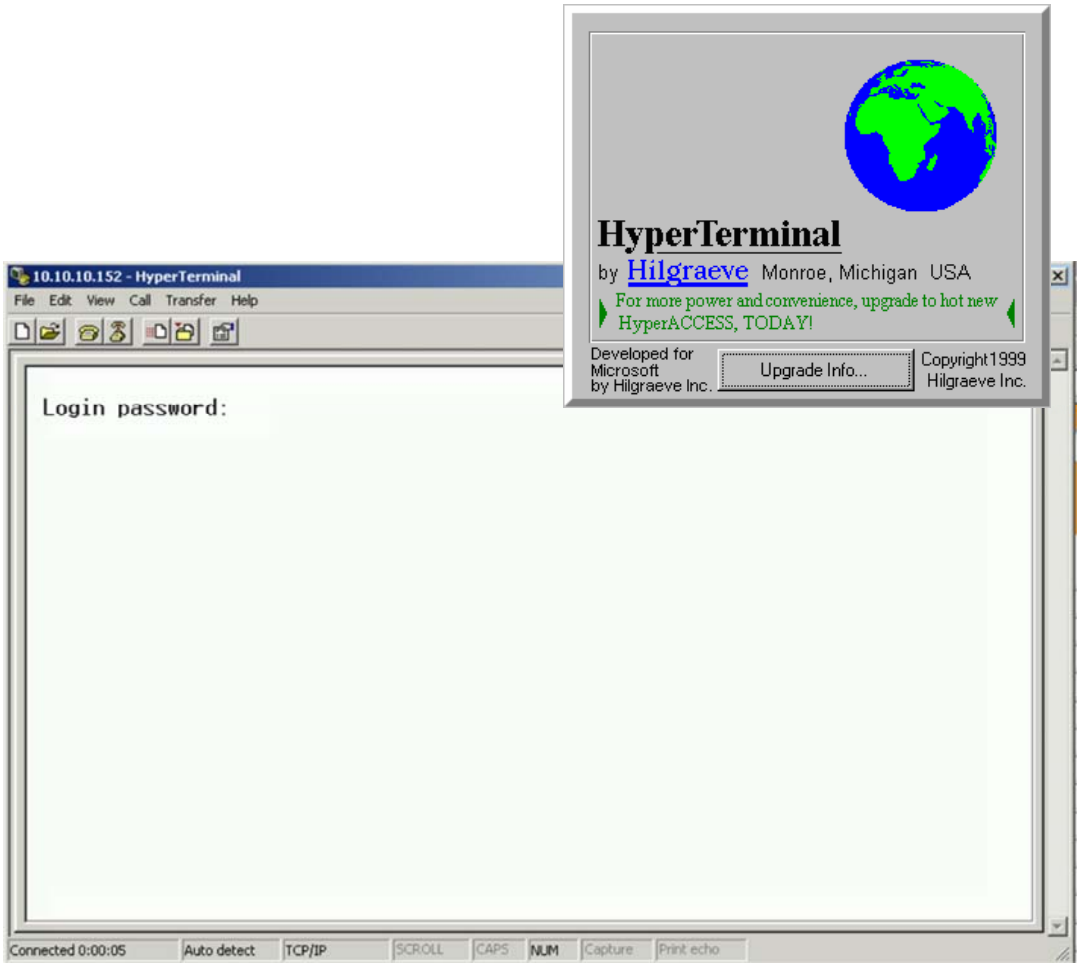
According to Example 1.

1. Any packets from/to inner IP 10.10.10.23 will have the bandwidth from 30% to 100%(priority 5). 30% is the guaranteed minimum bandwidth. If these packets do not use the guaranteed bandwidth, the bandwidth is given to other priority packets.
2. Any Web packets (with server inside or outside) will have the bandwidth from 30% to 50%(priority 7). 30% is the guaranteed minimum bandwidth. But the maximum bandwidth consumption will be limited to 50%. The web packets from/to 10.10.10.23 still have the bandwidth from 30% to 100%,

3. Any Ftp packets (with server inside or outside) from/to 10.10.10.10 ~ 10.10.10.200 will have the bandwidth from 0% to 100%(priority 9). This means that all these packets cannot get guaranteed bandwidth, but it can have up to 100% bandwidth if all the higher priority packets are not present.
4. Since the shaping condition 4 is meaningless; the bandwidth range of priority 11 is meaningless. But the guaranteed minimum bandwidth 30% will waste the total guaranteed bandwidth (total <= 100%).
5. Any other packets not satisfying these conditions will have the bandwidth from 0% to 100%(priority 10).

9.5 Run Telnet

Click this menu item will automatically run Telnet program and connect directly to the gateway system.



Steps:

- Click “Telnet” in left-side menu.

Notice:

The default Password for Telnet first stage login is “VoIP” and the second stage login is “antek”.

9.6 Help

This page will show you about help resources.

Steps:

- Click “Help” in left-side menu.

9.7 NAT Setting (VSP-5004/5002/WRG-5002/5004 only)

9.7.1 NAT Enable Control

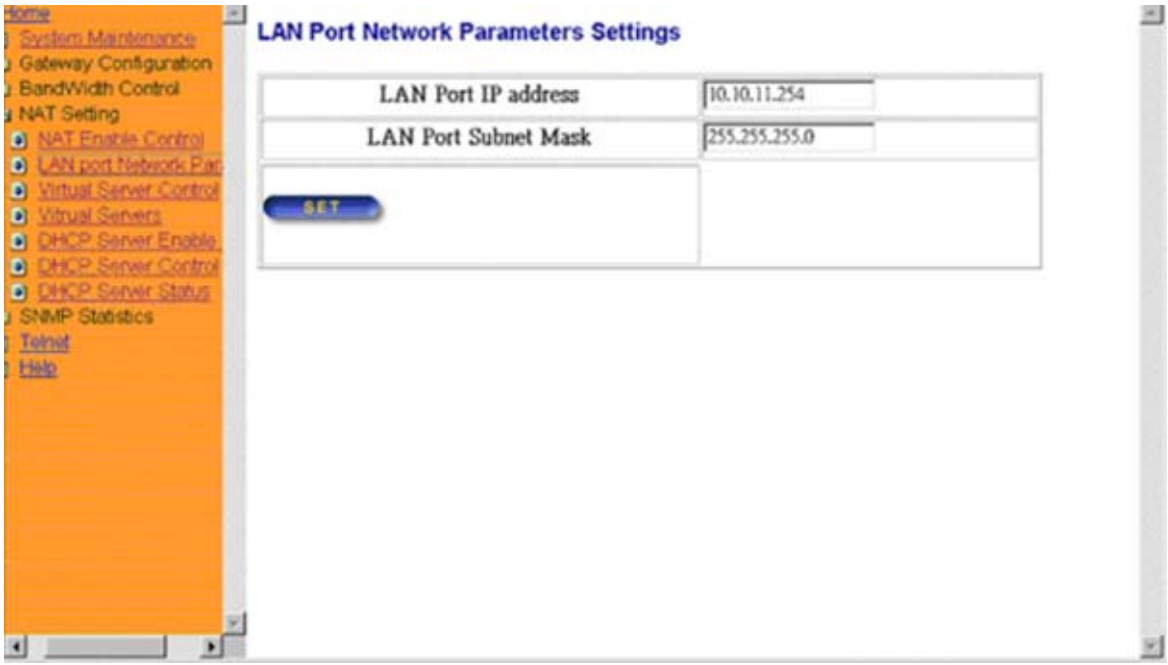
This page is for the setting to disable or enable the NAT function.

Steps:

- Click “NAT Enable Control” in left-side menu.
- Click “Enable NAT Function” or ”Disable NAT Function” selection.
- Press “SET” button.

9.7.2 LAN Port Network Parameters Settings

This page is for the setting of LAN port.



Steps:

- Click “LAN Port Network Parameter” in left-side menu.
- Enter the LAN Port IP Address.
- Enter the LAN Port Subnet Mask.
- Press “SET” button.

※ Default Router IP address: 10.10.11.254

※ PC’s individual IP address: 10.10.11.XXX (XXX can be the value: 1 to 253).

9.7.3 Virtual Server Control

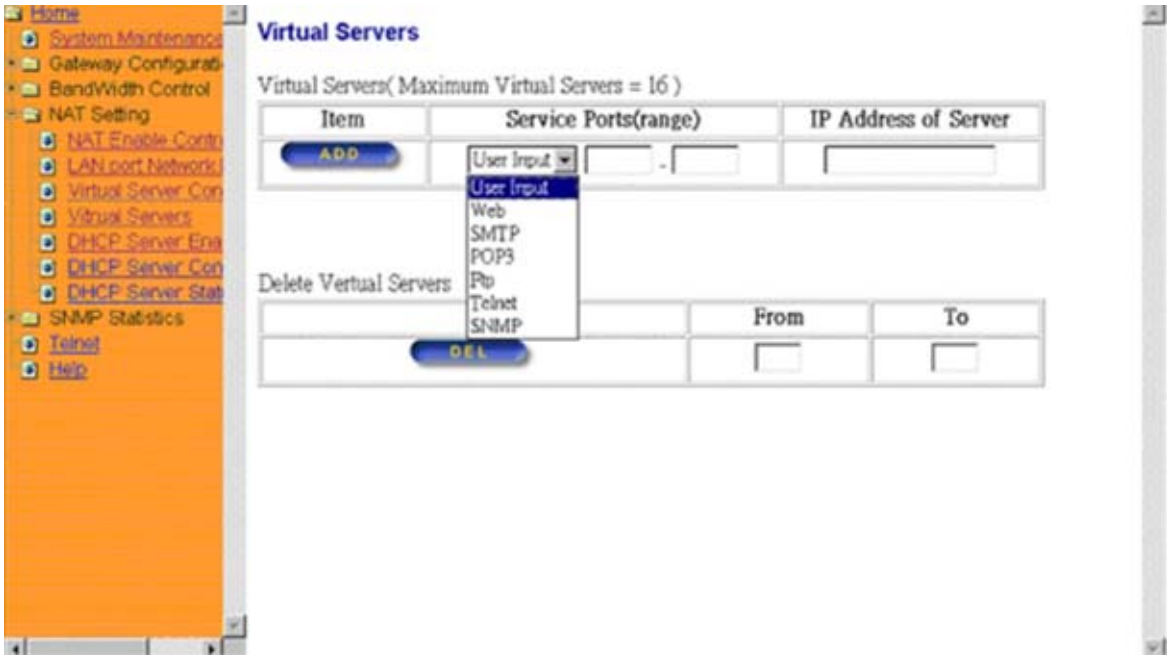
This page is for the setting to disable or enable the Virtual Server function.

Steps:

- Click “Virtual Server Control” in left-side menu.
- Click “Enable Virtual Servers ” or ”Disable Virtual Servers” selection.
- Press “SET” button.

9.7.4 Virtual Servers

This page is for the setting the Virtual Servers function.



Steps:

- Click “Virtual Servers” in left-side menu.
- Click the selection button of the Service-Ports to select the types of port range, they are divided into well known ports, such as Web/FTP/POPS/… , or User-Input ports which may be any port input by user.
- Input the beginning port and ending port if you select the User-Input type.
- Input the IP Address in the LAN side for the virtual server corresponding these ports.
- Press “ADD” button to add your setting into this configuration.
- Continually add the virtual-servers into your the configuration.
- If you want to delete any item, Press “DEL” button with the correct input of From-Item and To-Item.

9.7.5 DHCP Enable Control Mode

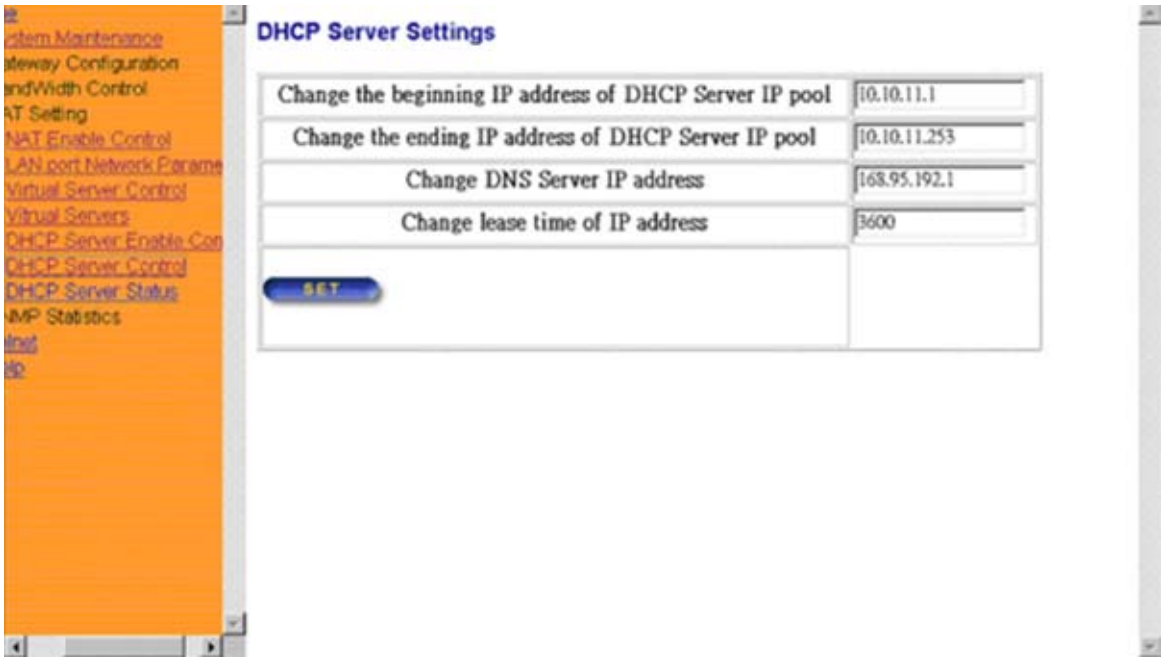
This page is for the setting to disable or enable the DHCP Server function.

Steps:

- Click “DHCP Server Enable Control” in left-side menu.
- Click “Enable DHCP Server Function ” or ”Disable DHCP Server Function” selection.
- Press “SET” button.

9.7.6 DHCP Server Control

This page is for the setting of DHCP Server.

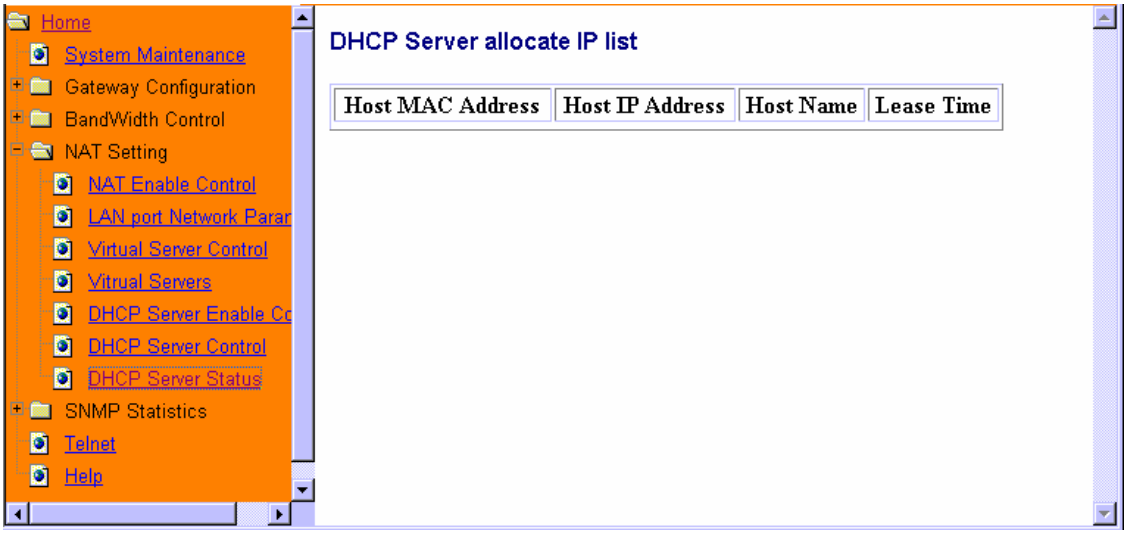


Steps:

- Click “DHCP Server Control” in left-side menu.
- Enter the IP address for “The beginning IP address of DHCP Server IP pool”.
- Enter the IP address for “The ending IP address of DHCP Server IP pool”.
- Enter the IP address for DNS server.
- Enter the lease time of IP address (unit in seconds: 3600 means 3600 seconds).
- Press “SET” button.

9.7.7 DHCP Server Status

This page will show the client information of DHCP Server.



9.8 Q.931 and RAS port number adjustment (Telnet / Console setting only)

The default Q.931 port number was 1720 and RAS port was 1719. When you need to change these two ports numbers to meet the network environment. You could select item "2" in main menu and select item "6" to change the RAS port, or select item "7" to change Q.931 port.

Steps:

In Main Menu, Please key in "2"
Key in 1 - i: 2

1. Set Default VoIP protocol.
2. Change The Gateway's H323-ID.
3. Change GateKeeper's IP address.
4. Change GateKeeper ID.
5. Change Prefix Address(Hunting).
6. Change Gatekeeper's RAS port.
7. Change Gateway's Q.931 port.

'ESC' to Upper Menu
Choose one item(1 - 7) : 6
Enter the Gatekeeper's RAS port number : xxxx *(Key in the RAS port number which you want)*
Choose one item(1 - 7) : 7
Enter the Gateway's Q.931 port number : xxxx *(Key in the Q.931 port number which you want)*

9.9 Wireless LAN Access Point Setting (WRG-5000 series devices only)

The WRG-5000 series devices provide Wireless Access Point function. You should set the SSID, WEP digits and communication channels.

Steps:

- Click “Wireless Setting ” in left-side menu.
- Input the characters in “SSID”.
- Select Encryption Method “Disable”, “64 bit” and “128 bit”
- Select the assigned channel from 1 ~11
- Press “SET” button.

Feedback

antek welcomes feedback both on Gateway and on the documentation.

Feedback on the Gateway

If you have any comments or suggestions about this product, please contact us, giving:

- The product name
- A concise explanation of your comments.

Feedback on this document

If you have any comments on this document, please contact us, giving:

- The document title
- The document number
- The page number to which your comments refer
- A concise explanation of your comments

General suggestions for additions and improvements are also welcome.

HQ

Address:
7F-3, No. 3, Lane 99, Puding Rd., HsinChu 300, Taiwan, R.O.C.
TEL: +886-3-5160139
FAX: +886-3-5160193

Taipei office

Address:
6F, No. 316, Sec. 1, Neihu Rd., Neihu Chiu, Taipei 114, Taiwan, R.O.C.
TEL: +886-2-2797-0790
FAX: +886-2-2797-0821

Email: service@antek.com.tw
http://www.antek.com.tw

Size of setting data (Table 3.)

Setting Items	Maximum Size
Console/Telnet login Password	30 characters
Brower Administrator Password	19 characters
Set Line Port Hunting Group Number	19 characters
Set Line Port Connected PBX Extension Numbers	17 characters
Set the Leading Number to call PSTN line	9 characters
Set the PSTN Line Access Code (add ',' to wait one second)	19 characters
Set Port's Hot Line Number	19 characters
Direct Dial Leading Number	19 characters
Gateway's H323-ID	32 characters
Gatekeeper's ID	23 characters

Appendix A: Terminology Index

ACF
Admission Confirm message

ADSL
Asymmetric Digital Subscriber Line

BRQ
Bandwidth Request

CDR
Call Detail Records

Codec:
The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are four kinds of Codec available; they are G.723, G.729, G.711_u and G.711_A. The default value is G.723.

DHCP
Dynamic Host Configuration Protocol

DSP
Digital Signal Processor

DTMF
Dual Tone Multiple Frequency. Dialing signals transmitted as two simultaneous voice band tones.

FTP
File Transfer Protocol

FXO port
Foreign Exchange Office port:
The FXO port is designed for connecting to PSTN line or a PBX line extension-side.

FXS port
Foreign Exchange Station (Subscriber) port: for connecting to the telephone set, fax machine, modem and conventional PBX.
The FXS port is designed for connecting to analog telephone set or a PBX trunk-side.

H.323

The ITU-T standard for sending the voice(audio) and video using IP on the Internet and within intranets.

IP

Internet Protocol

LAN

Local Area Network

MAC

The Medium Access Control (MAC) protocol is used to provide the data link layer of the Ethernet LAN system. The MAC protocol encapsulates a SDU (payload data) by adding a 14-byte header (Protocol Control Information (PCI)) before the data and appending a 4-byte (32-bit) Cyclic Redundancy Check (CRC) after the data. The entire frame is preceded by a small idle period (the minimum inter-frame gap, 9.6 microsecond (μS)) and an 8-byte preamble.

MIS

Management Information System

NAT

Network Address Translation

PABX

Private Automatic Branch Exchange

PBX

Private Branch Exchange

PPPoE

Point-to-Point Protocol over Ethernet

PSTN

Public Switched Telephone Network

QoS

Quality of Service

RTP

Real Time Transfer Protocol

RTCP

Real Time Transfer Control Protocol

RRQ

Registration Request (for IP address, phone number, etc)

SNMP
Simple Network Management Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

TOS
Type of Service

UTP
Unshielded Twisted Pair

VoIP
Voice over Internet Protocol. Transmit voice signals as packets over TCP/IP networks.

WAN
Wide Area Network

Appendix B: Specification

Protocol and Standard
ITU H.323 v2/v3/v4 compliant
RFC 2543 SIP compliant
TCP/IP, RTP, HTTP, Telnet, DHCP, PPPoE
Voice Processing
ITU G.711/64kbps, G.723.1A/5.3,6.3kbps, G.729A/B/8kbps
Voice Activity Detection (VAD)
Comfort Noise Generation (CNG)

Tone Generation and Detection
TIA-464B DTMF, Dial, Busy, Ring Back, Call Progress.

FAX Relay
T.30/T.38 real-time FAX compliant.
Voice/FAX auto-switch.

Echo Cancellation
G.165/G.168 with 8-16ms echo tail.

Software Upgrade
FTP/TFTP

PSTN Interface
EGW-802: 2 FXO ports
EGW-802S: 2 FXS ports
EGW-802A: 1 FXS port + 1 FXO port
EGW-804: 4 FXO ports
EGW-804S: 4 FXS ports
EGW-804A: 2 FXO + 2 FXS ports
EGW-804B: 1 FXS + 3 FXO ports
EGW-804C: 3 FXS + 1 FXO ports
VSP-2500: 1 to 4 analog PSTN modules. Each module offers 4 analog ports.
VM-402: 4 FXO ports module
VM-401S: 4 FXS ports module
VM-442S: 2 FXO + 2 FXS ports module
VSP-5002: 2 FXO ports
VSP-5002S: 2 FXS ports
VSP-5002A: 1 FXS port + 1 FXO port
VSP-5004 /GK: 4 FXO ports
VSP-5004S /SGK: 4 FXS ports
VSP-5004A: 2 FXO + 2 FXS ports
VSP-5004B: 3 FXO + 1 FXS ports

VSP-5004C: 1 FXO + 3 FXS port
WRG-5002: 2 FXO ports
WRG-5002S: 2 FXS ports
WRG-5002A: 2 FXO + 2 FXS ports
WRG-5004: 2 FXO + 2 FXS ports
WRG-5004S: 2 FXO + 2 FXS ports
WRG-5004A: 2 FXO + 2 FXS ports
WRG-5004B: 2 FXO + 2 FXS ports
WRG-5004C: 2 FXO + 2 FXS ports

Network Interface
EGW Series:
1 Ethernet ports for LAN
10Base-T and 100Base-T, IEEE802.3 compatible
VSP Series:
2 Ethernet ports, one for LAN, one for WAN (VSP-5002 series)
5 Ethernet ports, four for LAN, one for WAN (VSP-5004 series)
10Base-T and 100Base-T, IEEE802.3 compatible
WRG Series**:**
2 Ethernet ports, one for LAN, one for WAN (WRG-5002 series)
5 Ethernet ports, four for LAN, one for WAN (WRG-5004 series)
10Base-T and 100Base-T, IEEE802.3 compatible
One Access Point was Built In.

Console
RS-232, DB9

LED Indicators
LAN: 10/100M, Collision, Link, Active (Tx/Rx)
WAN: 10/100M, Collision, Link, Active (Tx/Rx)
Line (off-hook/ringing)
Phone (off-hook/ringing)
Power

Power
100~240V AC, 50~60 Hz
Environmental
Humidity: 10~90%, non-condensing
Operating temp: 0~50 degrees C
Storage temp: -10~70 degrees C

Dimension
1U:
VSP-2500: 440mm (L) x 255mm (W) x 44mm (H)

Compact:

EGW-802:	190mm (L) x 110mm (W) x 35mm (H)
EGW-804:	240mm (L) x 165mm (W) x 36mm (H)
VSP-5002:	190mm (L) x 110mm (W) x 35mm (H)
VSP-5004:	240mm (L) x 165mm (W) x 36mm (H)
WRG-5002:	240mm (L) x 110mm (W) x 35mm (H)
WRG-5004:	290mm (L) x 165mm (W) x 36mm (H)

Weight

VSP-2500:	4.4Kg
EGW-802	0.7 Kg
EGW-804	0.7 Kg
VSP-5002	0.7 Kg
VSP-5004	0.7 Kg
WRG-5002	0.7 Kg
WRG-5004	0.7 Kg

Safety

UL1950, EN60950

EMC

FCC part 15 Class B, CE mark, VCCI, BSMI

Vibration and Drop

IEC 68-2-36, IEC 68-2-6, EC 68-2-32

Wireless Access Point (WRG-5002/5004 Series Devices only)

- Data Rates Supported: 802.11b: 1, 2, 5.5, 11 Mbps
- Frequency Band: 802.11b: 2.4 GHz
- Media Access Protocol: CSMA/CA
- Operating Channels: 802.11b : 1 – 11
- Operating Rang: 802.11b: up to 100 meters (328 feet) transmit and receive
- Security: 64- and 128- bit WEP encryption; ESSID; password protection
- Wireless Standards Conformance: Wi-Fi Certified and IEEE 802.11b
- Wireless Medium: DSSS